用主动免疫可信计算保障信创产业高质健康发展

国家集成电路产业发展咨询委员会委员
中央网信办专家咨询委员会顾问
国家三网融合专家组成员
沈昌祥　院士

机遇与挑战

中共中央政治局近期密集召开会议，列入今年政府工作报告，部署统筹做好疫情防控和经济社会发展，要求以科技产业为突破口，加快推动5G网络、数据中心、工业互联网等新型基础设施建设进度。“新基建”作为国家经济发展战略，正在显现出强大动能，聚焦新旧动能转换，助力信创产业迈向新高度。但对网络安全也提出了严重挑战，必须有效应对垄断网络空间霸权威慑，筑牢网络安全防线。

1

PART

主动免疫可信计算保障新基建健康发展

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，也是国际战略在军事领域的演进，我国的网络安全正在面临着严峻挑战。“没有网络安全就没有国家安全”，按照国家网络安全法律、战略和等级保护制度要求，推广安全可信产品和服务，筑牢网络安全底线是历史的使命。新型基础设施是以数据和网络为核心，其发展前提是用主动免疫的可信计算筑牢安全防线。

案例： 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，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，造成约十几亿美元的营业损失。最近的5.4侠盗版危害极大。

《网络安全法》

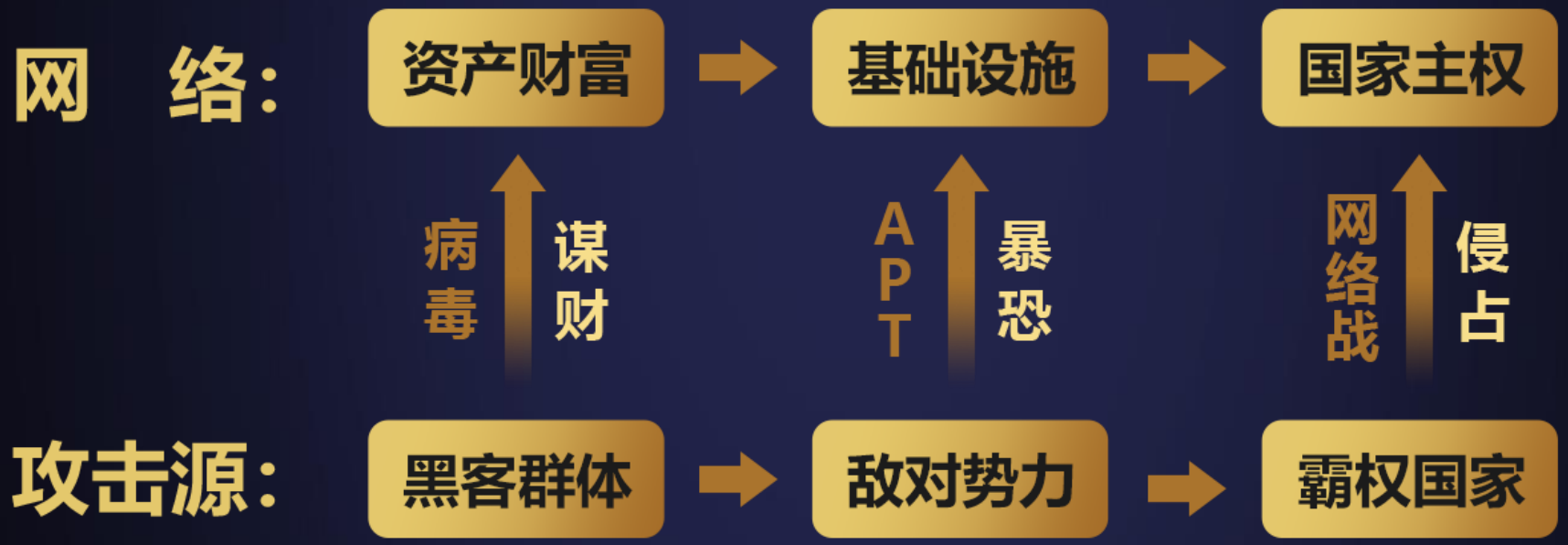
第十六条 国务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，**推广安全可信的网络产品和服务**，保护网络技术知识产权，支持企业、研究机构和高等学校等参与国家网络安全技术创新项目。

《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。

安全风险的实质及对策

网络空间极大威胁：有利可图、全方位攻击



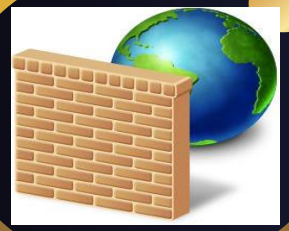
网络空间极其脆弱

是

- 计算科学问题 ------- 图灵计算原理（少攻防理念）
- 体系结构问题 ------- 冯诺伊曼架构（缺防护部件）
- 计算模式问题 ------- 重大工程应用（无安全服务）

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。

主动免疫的计算目标：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。相当于人体具有主动免疫功能使得其能健康生活。



防火墙

病毒查杀

入侵检测

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。

2

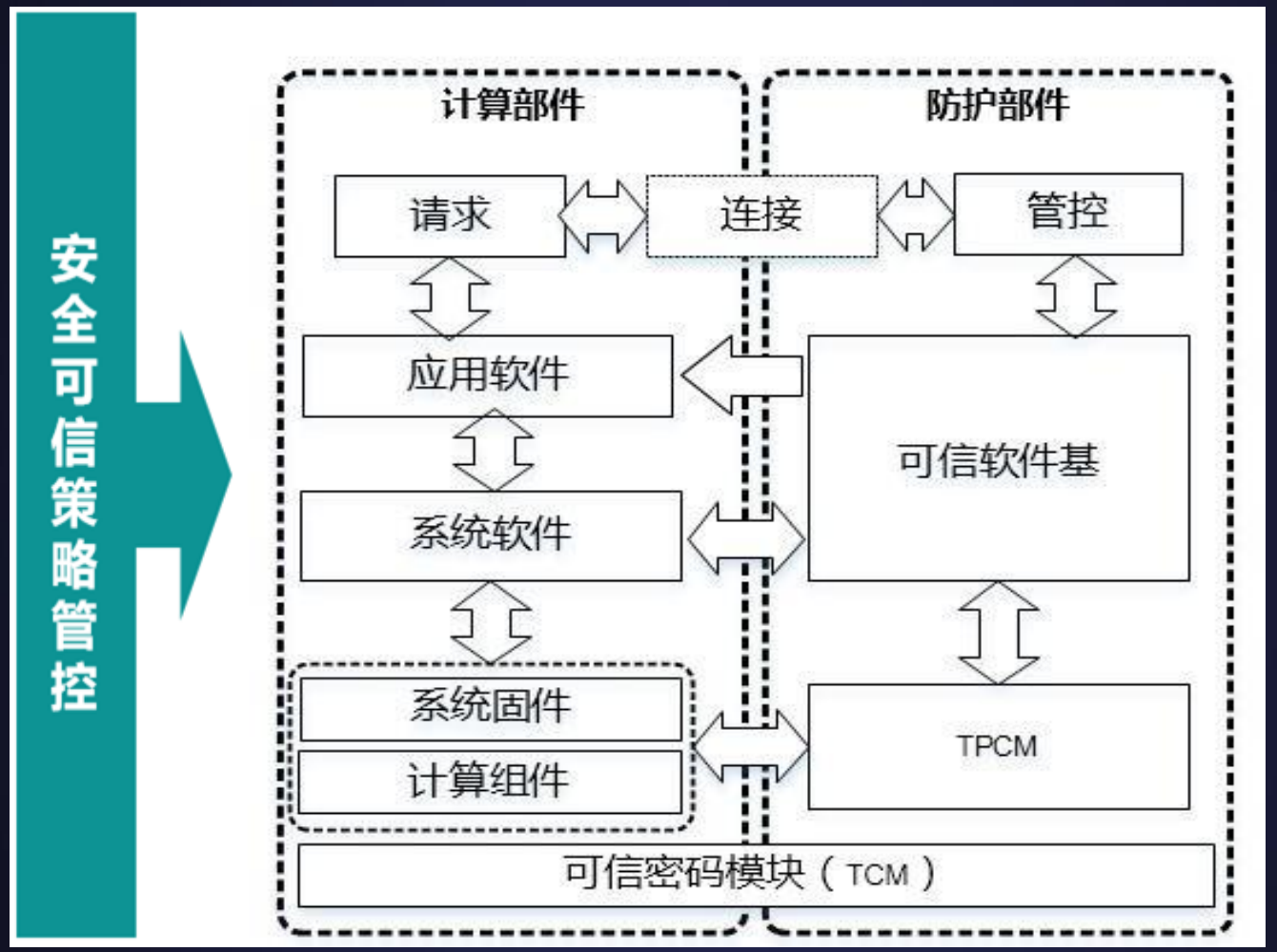
PART

构建新基建网络安全主动免疫新体系

1、“一种”新模式 计算同时进行安全防护

主动免疫可信计算是一种运算同时进行安全防护的**新计算模式**，**以密码为基因抗体**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。

2、“二重”体系结构 计算部件+防护部件

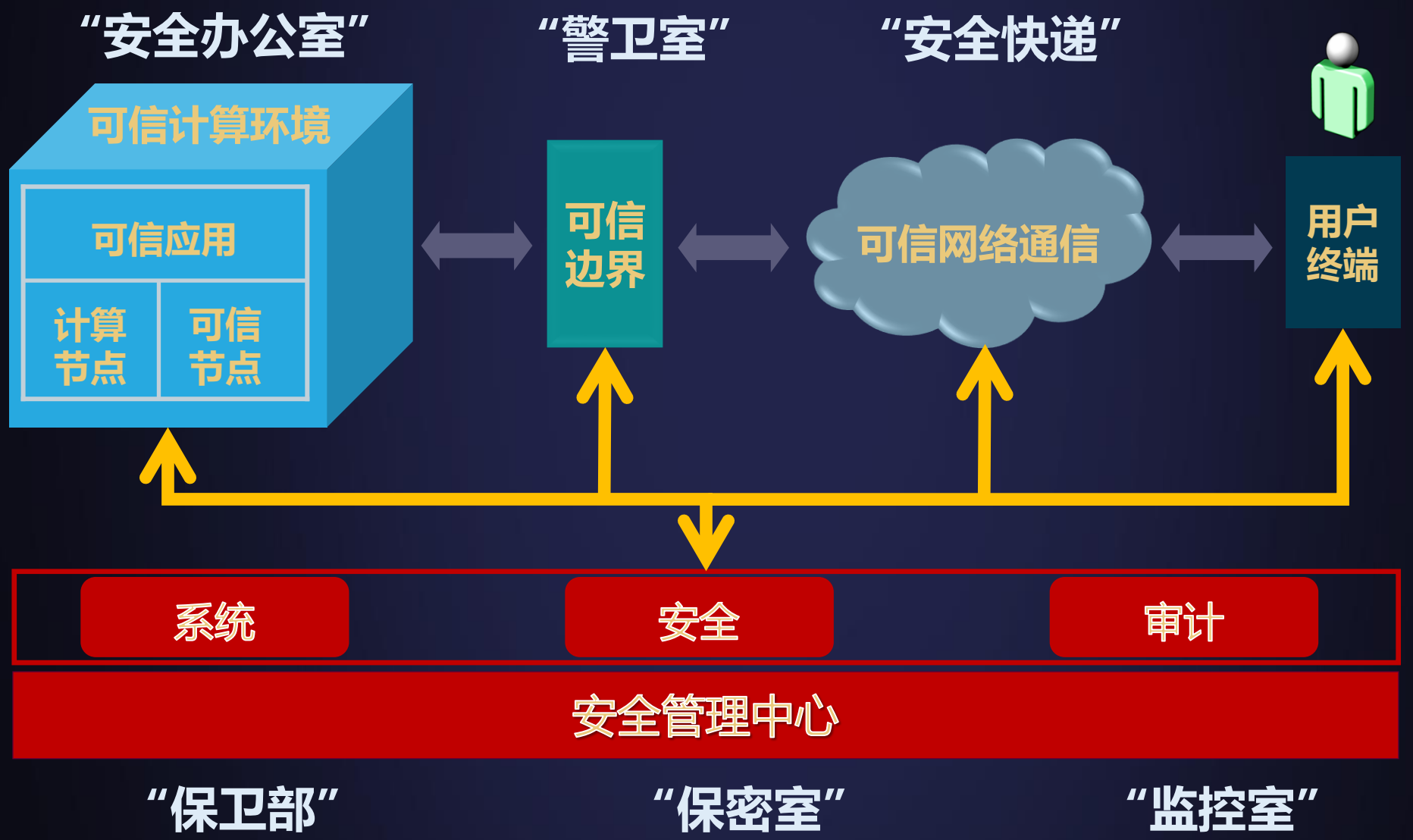


建立免疫 反腐败子系统

二重体系结构的可信计算节点

3、“三重”防护框架

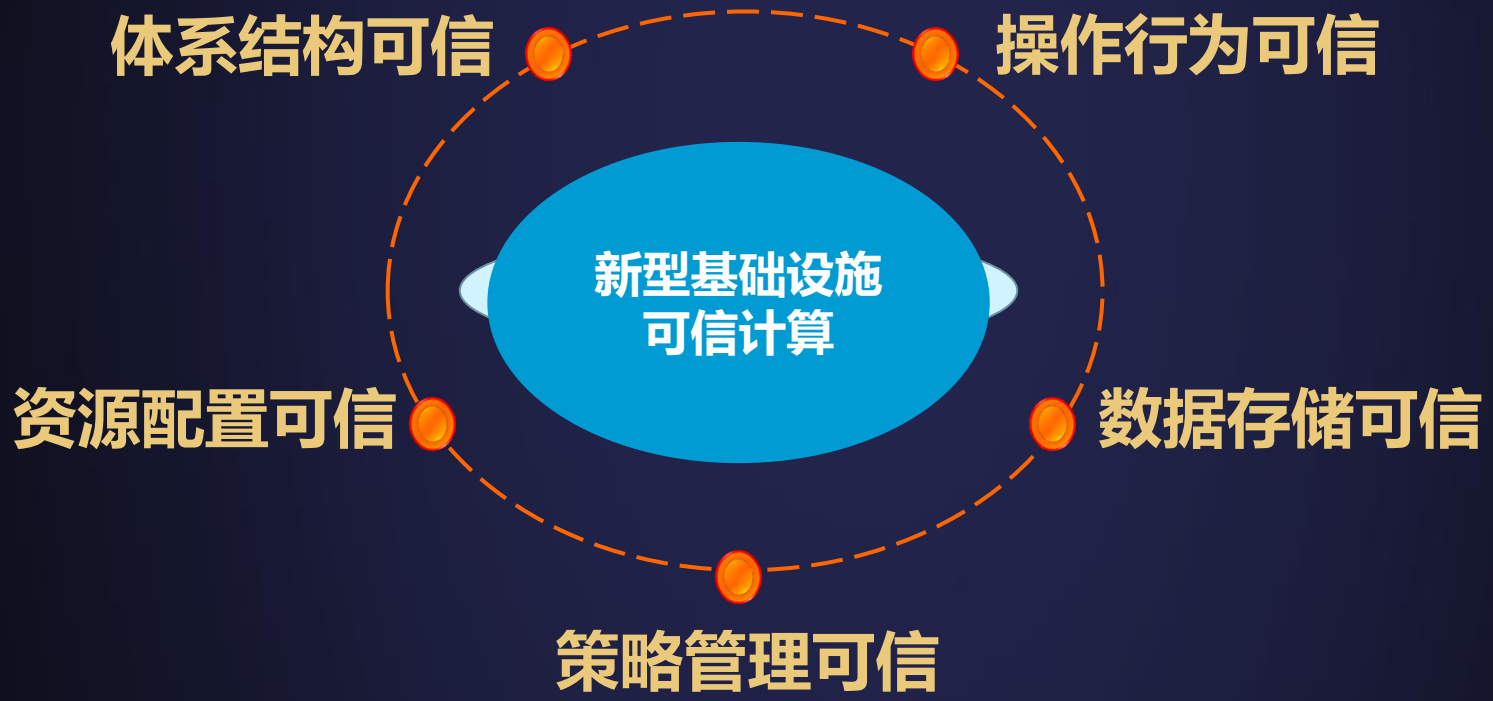
可信安全管理中心支持下的主动免疫三重防护框架



4、“四要素”人机可信交互

人机交互可信是发挥5G、数据中心等新基建动能作用的源头和前提，必须对人的操作访问策略四要素（主体、客体、操作、环境）进行可信度量、识别和控制，纠正了传统的访问控制策略模型只基于授权标识属性进行操作，而不作可信验证，难防篡改的安全缺陷。

5、“五环节”可信设施 加强基础设施全程安全管控，用可信密码等技术检测确保设施各环节安全可信



6、“六不”防护效果

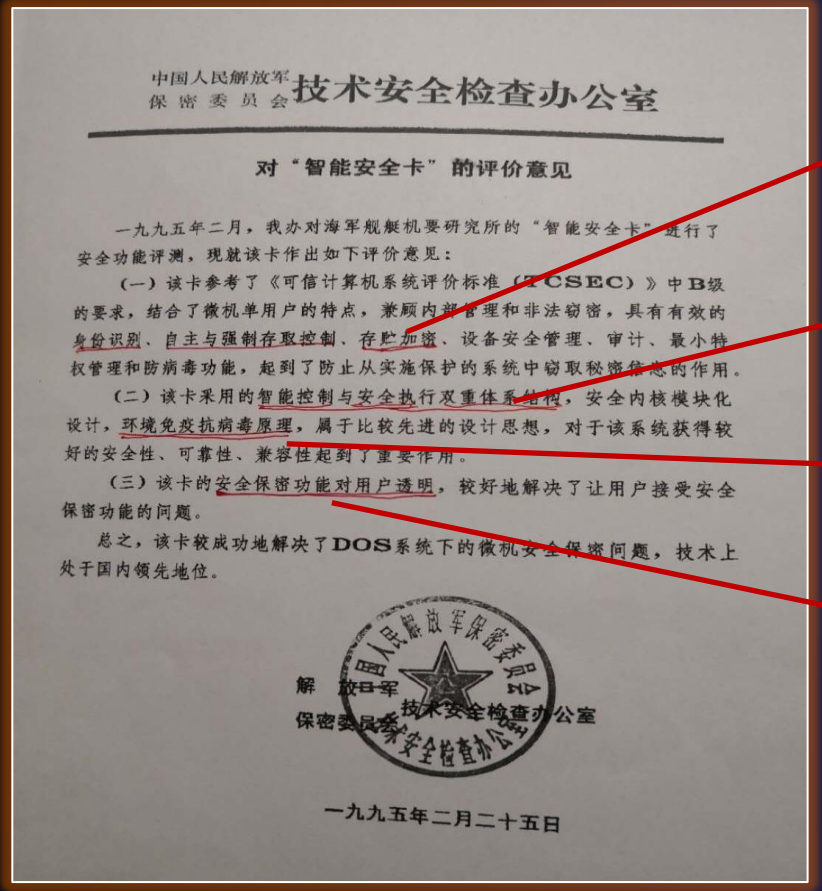
“WannaCry”、“Mirai”、“黑暗力量”、“震网”、“火焰”、“心脏滴血”等不查杀而自灭

3

PART

建造安全可信自主创新的新型产业空间

中国可信计算源于1992年立项研制**免疫的综合安全防护系统（智能安全卡）**，于1995年2月底通过测评和鉴定。经过长期军民融合攻关应用，形成了自主创新安全可信体系，开启了**可信计算3.0时代。**



中国人民解放军保密委员会技术安全检查办公室

对“智能安全卡”的评价意见

一九九五年二月，我办对海军舰艇机要研究所的“智能安全卡”进行了安全功能评测，现就该卡作出如下评价意见：

（一）该卡参考了《可信计算机系统评价标准（TCSEC）》中B级的要求，结合了微机单用户的特点，兼顾内部管理和非法窃密，具有有效的身份识别、自主与强制存取控制、存贮加密、设备安全管理、审计、最小特权管理和防病毒功能，起到了防止从实施保护的系统中窃取秘密信息的作用。

（二）该卡采用的智能控制与安全执行双重体系结构，安全内核模块化设计，环境免疫抗病毒原理，属于比较先进的设计思想，对于该系统获得较好的安全性、可靠性、兼容性起到了重要作用。

（三）该卡的安全保密功能对用户透明，较好地解决了让用户接受安全保密功能的问题。

总之，该卡较成功地解决了DOS系统下的微机安全保密问题，技术上处于国内领先地位。

中国人民解放军保密委员会技术安全检查办公室

一九九五年二月二十五日

公钥密码身份识别、对称密码加密存储

智能控制与安全执行双重体系结构

环境免疫抗病毒原理

数字定义可信策略对用户透明

开创可信计算3.0时代

求是

用可信计算构筑网络安全

■ 中国工程院院士 沈昌祥

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，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。习近平总书记强调，建设网络强国，要有自己的技术，有过硬的技术。解决信息化核心技术设备受制于人的问题，需要从计算模式和体系结构上创新驱动。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”网络强国的重要举措。

一、可信可用方能安全交互

网络空间的安全与人类社会休戚相关。在人类社会中，信任是人们相互合作和交往的基础，如果我们确定对方不可信，就不会与其合作和交往。网络空间由于其开放性，允许两个网络实体未经过任何事先的安排或资格审查，就可以进行交互。这就导致我们在进行交互时有可能对对方实体一无所知。对方实体可能是通

求是杂志 2015·20 33

中国共产党中央委员会主办 QIUSHI 2015·20

解读品牌竞争力 新华通讯社主管

CHINA TOP BRANDS 中国名牌

可信计算：网络安全的主动防御时代

可信计算技术及可信计算系统产业的出现，颠覆了人们以往对网络安全防护的认知，变“被动防御”为“主动防御”，让信息交互平台中最脆弱可靠的信任基础与信任保障，驶上高速信息安全的快车道。

沈昌祥：可信计算让信息系统国产化真正落地

Shen Changxiang: Trusted Computing Ensure That The Information System Localization Takes Effect

本刊记者 / 杨侠 摄影 / 王楚天

Windows系统升级的背后，有着怎样的可信计算机制较量？可信计算究竟是怎样的一种信息安全保障模式，在自主可控信息系统国产化战略中又能起到怎样的作用？带着这些问题，记者特别专访了信息安全领域权威专家、中国工程院院士沈昌祥。

的密码就相当于人体的基因，对于“基因”的变异可用编码原理检验其有无变化。可信计算的免疫功能就像人体的免疫功能一样，是一个动态的支撑体系，可独立成为一个循环系统，进行完整性检查。换言之，

中国工程院院士沈昌祥（左）讲述可信计算的研究与应用

◆可信可用方能安全交互

◆主动免疫方能有效防护

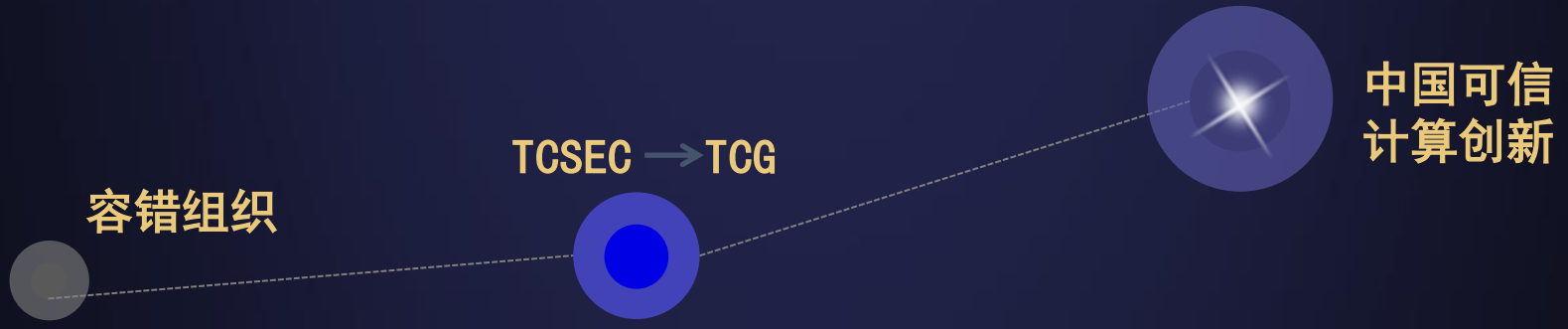
◆自主创新方能安全可控

新华社 《中国名牌》

可信计算：网络安全的主动防御时代

开创可信计算3.0新时代

	可信1.0（主机）	可信2.0（PC）	可信3.0（网络）
特性	主机可靠性	节点安全性	公钥、对称双密码主动系统免疫
对象	计算机部件	PC单机为主	终端、服务器、存储系统体系可信
结构	冗余备份	功能模块	宿主+可信双节点平行架构
机理	故障诊查	被动度量	基于网络可信服务验证
形态	容错算法	TPM+TSS	动态度量实时感知
	世界容错组织为代表	TCG为代表	中国为代表



《国家中长期科学技术发展（2006-2020年）》明确提出“以发展高可信网络为重点，开发网络安全技术及相关产品，建立网络安全技术保障体系”。

可信计算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、中央电视台全数字化可信制播环境建设、国家电网电力数字化调度系统安全防护建设，已成为国家法律、战略、等级保护制度要求进行推广应用，其密码体制和体系结构等5大核心技术已被世界著名企业和机构所采用，俄罗斯卡巴斯基最近宣布不搞杀病毒软件而要建免疫网络，美国防部热推“零信任架构”等都是异曲同工之举。

完备的可信计算3.0产品链，将形成巨大的新型产业空间

自主可信计算平台产品设备有三种形态：

- 系统重构可信主机
- 主板配插PCI可信控制卡
- 配接USB可信控制模块

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。

4

PART

按等级保护制度要求化解网络安全风险

1、等保2.0新标准把云计算、移动互联网、物联网和工控等采用可信计算3.0作为核心要求，筑牢网络安全防线

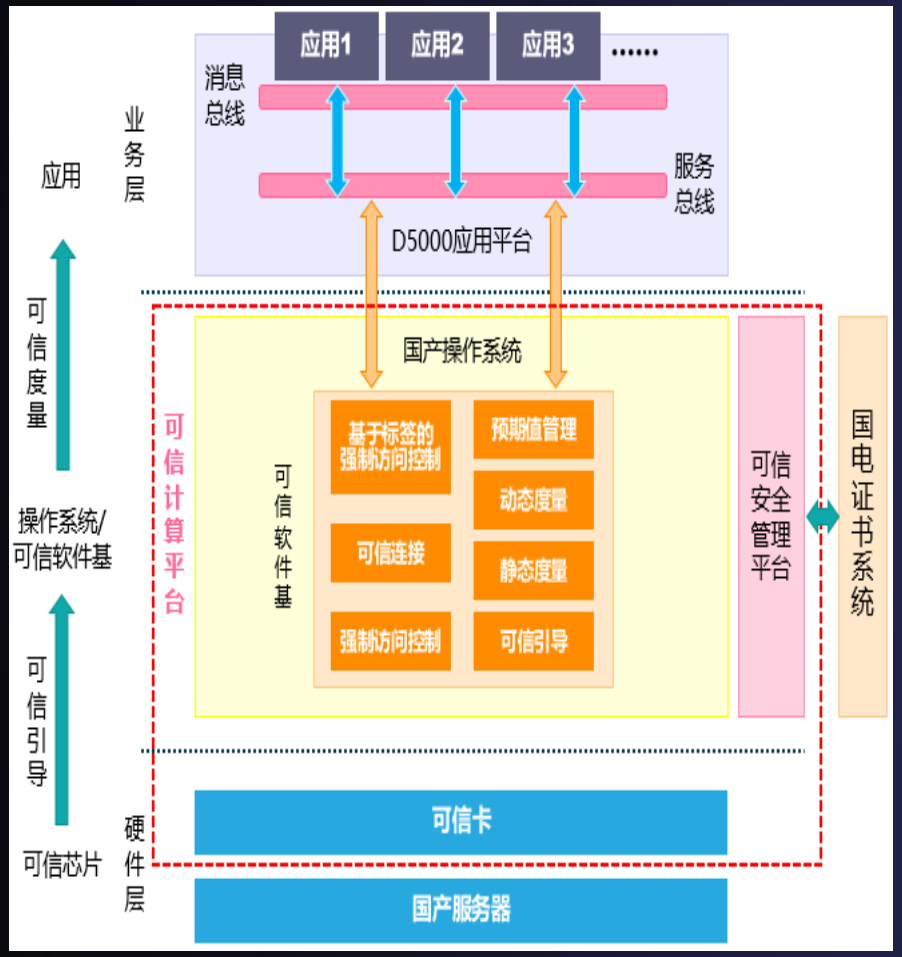
	一级	二级	三级	四级
等级保护标准可信计算要求	所有计算节点都应基于可信根实现开机到操作系统启动的可信验证。	所有计算节点都应基于可信根实现开机到操作系统启动，**再到应用程序启动**的可信验证。**并将验证结果形成审计纪录。**	所有计算节点都应基于可信根实现开机到操作系统启动，再到应用程序启动的可信验证，**并在应用程序的关键执行环节对其执行环境进行可信验证，主动抵御入侵行为。**并将验证结果形成审计纪录，**送到管理中心。**	所有计算节点都应基于可信计算技术实现开机到操作系统启动，再到应用程序启动的可信验证，并在应用程序的**所有**执行环节对其执行环境进行可信验证，主动抵御入侵行为。并将验证结果形成审计纪录，送到管理中心，**进行动态关联感知，形成实时的态势。**

可信宿主	TCM	TPCM	检验软件	可信软件基（TSB）		
	静态可信验证基础软件可信			建链检验 应用程序可信	动态度量 执行环境	实时感知 关联态势
	BIOS	引导OS，装载系统		应用加载	应用执行	所有执行
	一级			二级	三级	四级

2、国家电网电力调度系统安全防护建设

发改委14号令决定以可信计算架构实现等级保护四级。

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。



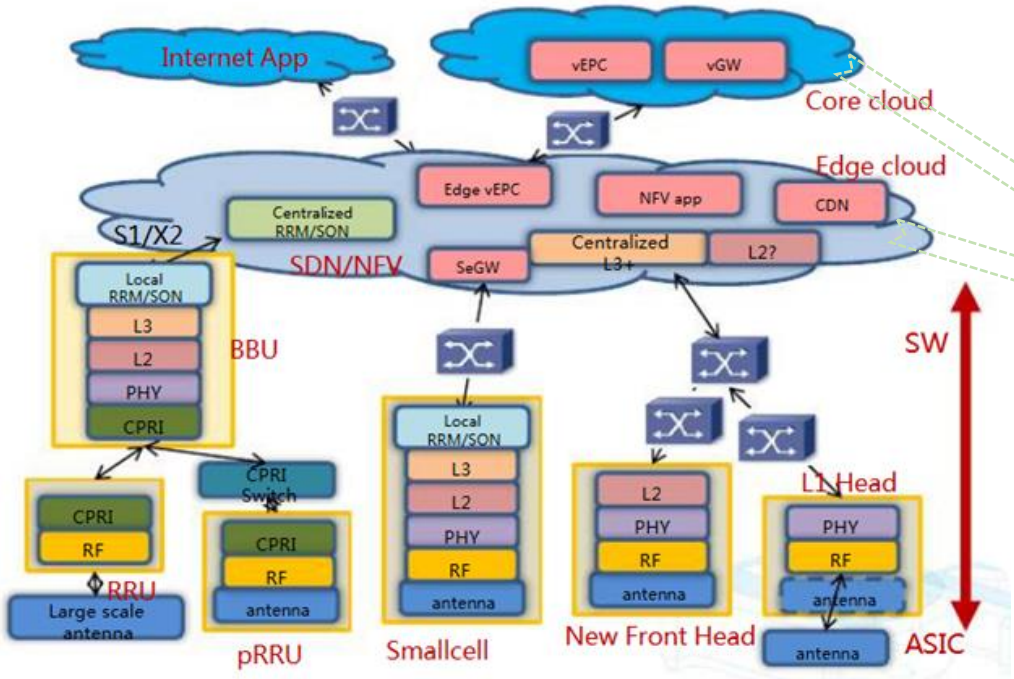
国家电网电力调度系统安全架构

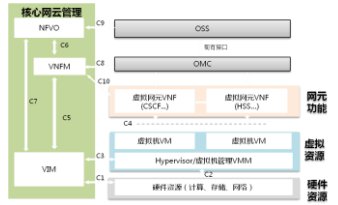
- 高效处理：实时调度
- 不打补丁：免疫抗毒
- 不改代码：方便实施
- 精练消肿：降低成本

3、新型基础设施标准安全架构

5G网络设施等保新标准安全架构

5G网络在传统电信云的基础上引入**NFV/SDN**等技术进行ICT融合，将移动通信网络**云化**、**虚拟化**和**软件化**，使网络变得更灵活、敏捷和开放。



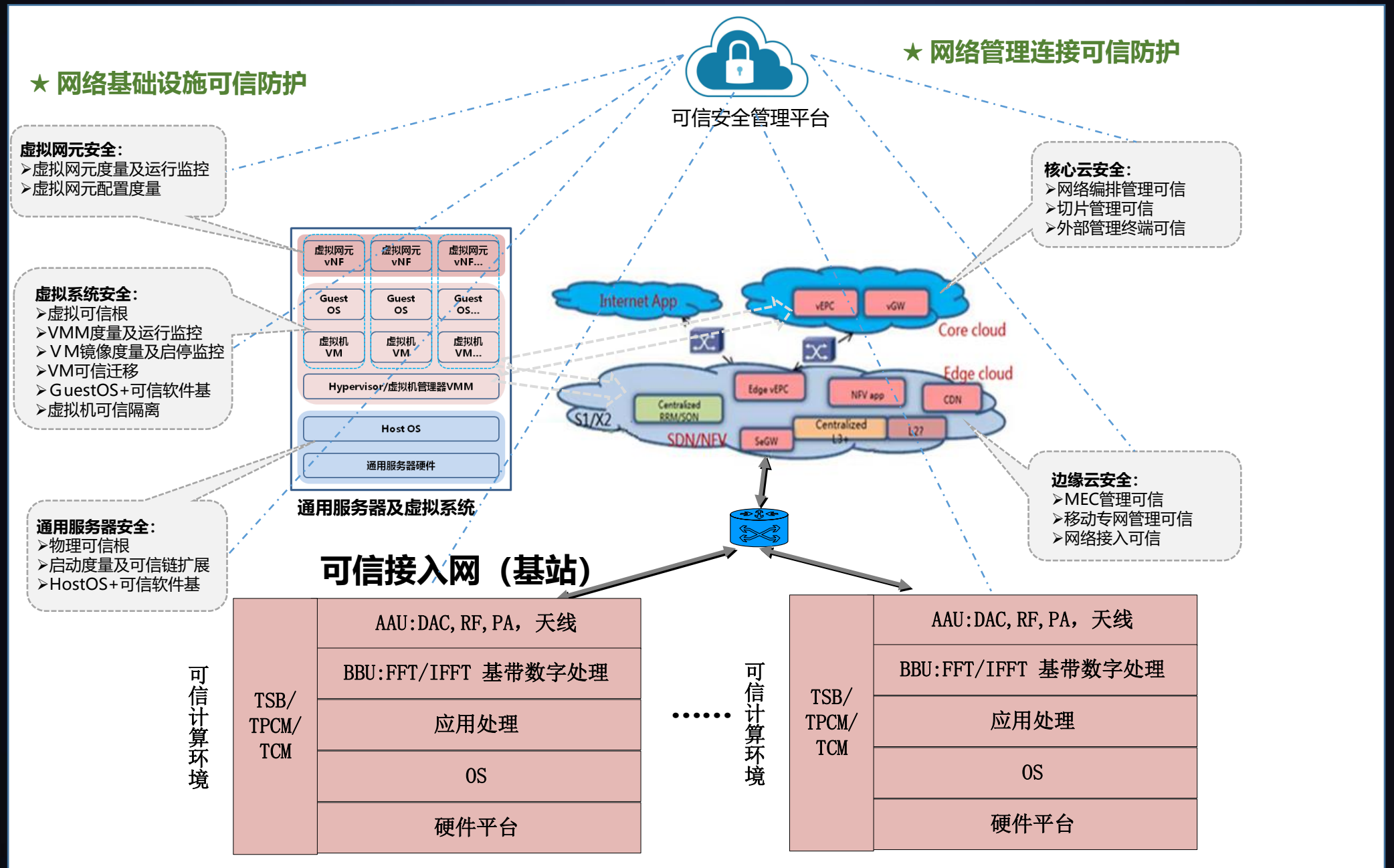


虚拟化软件及网元

通用服务器

在5G网络的核心云和边缘云中传统的网络设备将被**通用服务器**及**虚拟化网元**软件所代替

5G核心网络可信计算架构



谢　谢！