打造网络空间安全
可信主动免疫新生态

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

沈昌祥

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

“没有网络安全就没有国家安全 安全是发展的前提”

《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标准及“关基”条例要求应当优先采购全面使用安全可信的产品和服务来构建关键基础设施安全保障体系。

1 PART

以安全可信构筑网络主动免疫保障体系

网络空间面临严重威胁

（1）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。

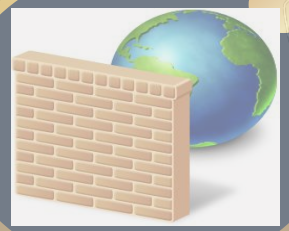
（2）2018年8月3日，台积电遭到勒索病毒入侵，几个小时之内，台积电在中国台湾地区的北、中、南三个重要生产基地全部停摆，造成约十几亿美元的营业损失。

（3）2021年5月7日，美国最大的成品油管道运营商Colonial Pipeline受到勒索软件攻击，被迫关闭其美国东部沿海各州供油网络，美国政府宣布美国17个州和华盛顿特区进入紧急状态。

从科学技术上认清安全风险本质：网络安全风险源于图灵机原理少攻防理念、冯·诺依曼结构缺防护部件和工程应用无安全服务的先天性脆弱缺陷。再加上认知科学的局限性，设计IT系统不能穷尽所有逻辑组合，必定存在大量未经处理的逻辑缺陷。因此，利用缺陷脆弱点挖掘漏洞进行威胁攻击是网络安全风险的永远命题。传统“封堵查杀”补丁难以应对未知恶意攻击。安全可信产品和服务是实施计算运算同时并行进行动态的全方位整体防护，使得能完成计算任务的逻辑组合不被篡改和破坏，达到预期的计算目标。相当于人体具有免疫力确保健康。由此，按国家网络安全法律、战略及等保制度要求以基础原理、核心技术和工程应用创新，用安全可信网络产品和服务构建主动免疫防护的保障体系。

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。



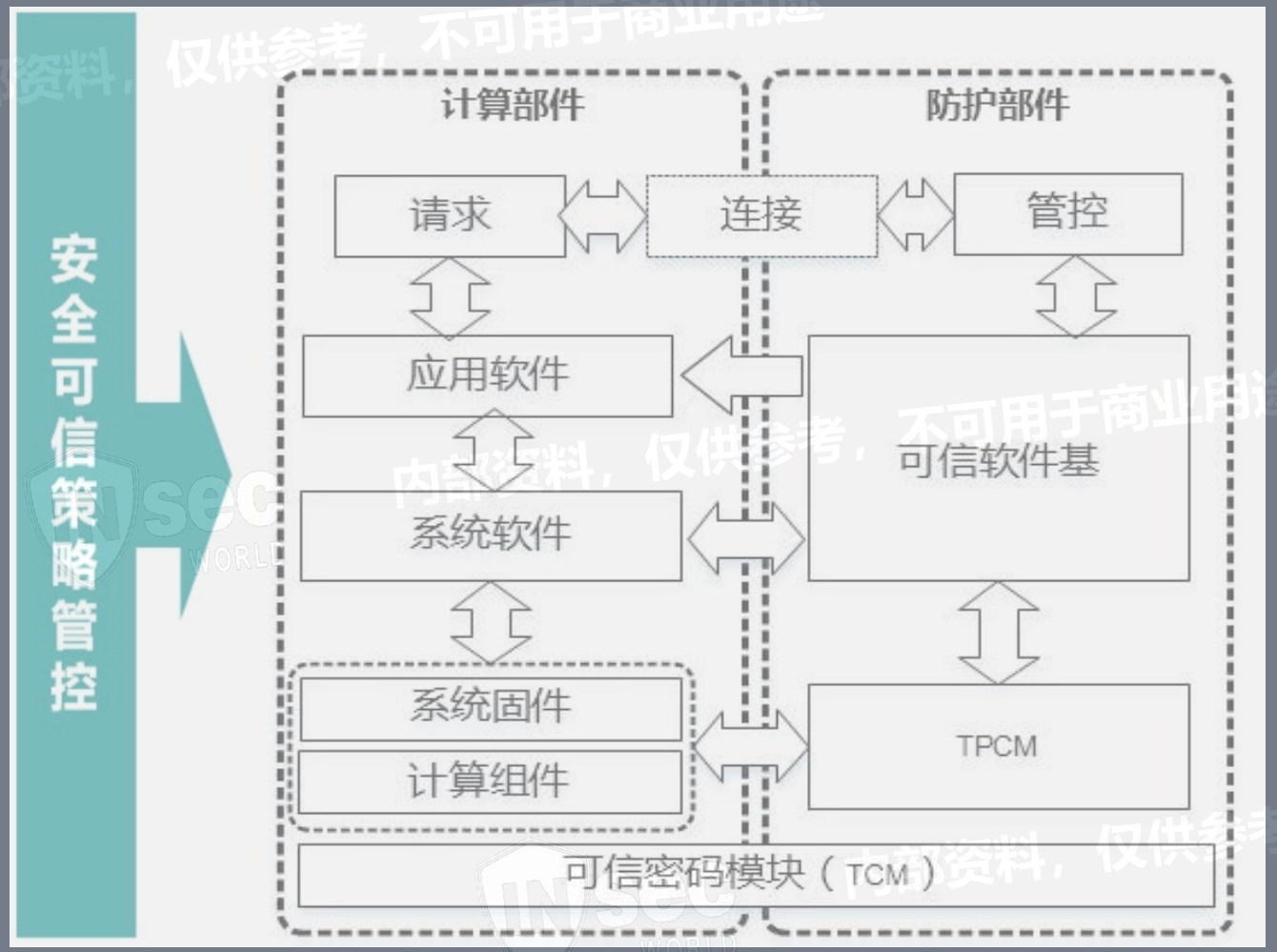
防火墙

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、“二重”体系结构 计算部件+防护部件



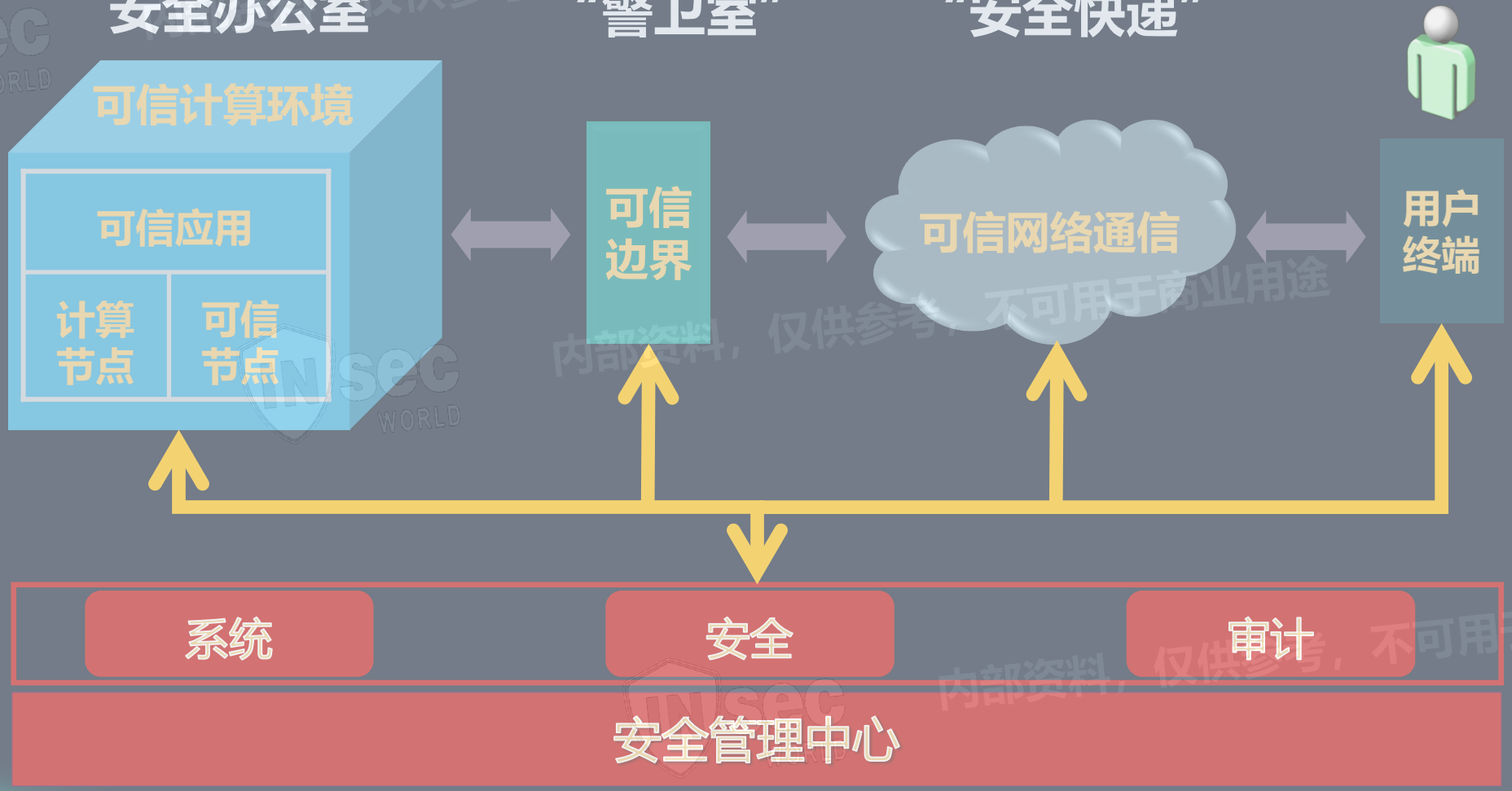
二重体系结构的可信计算节点

建立免疫、反腐败子系统

3、“三重”防护框架 系统工程

可信安全管理中心支持下的主动免疫三重防护框架

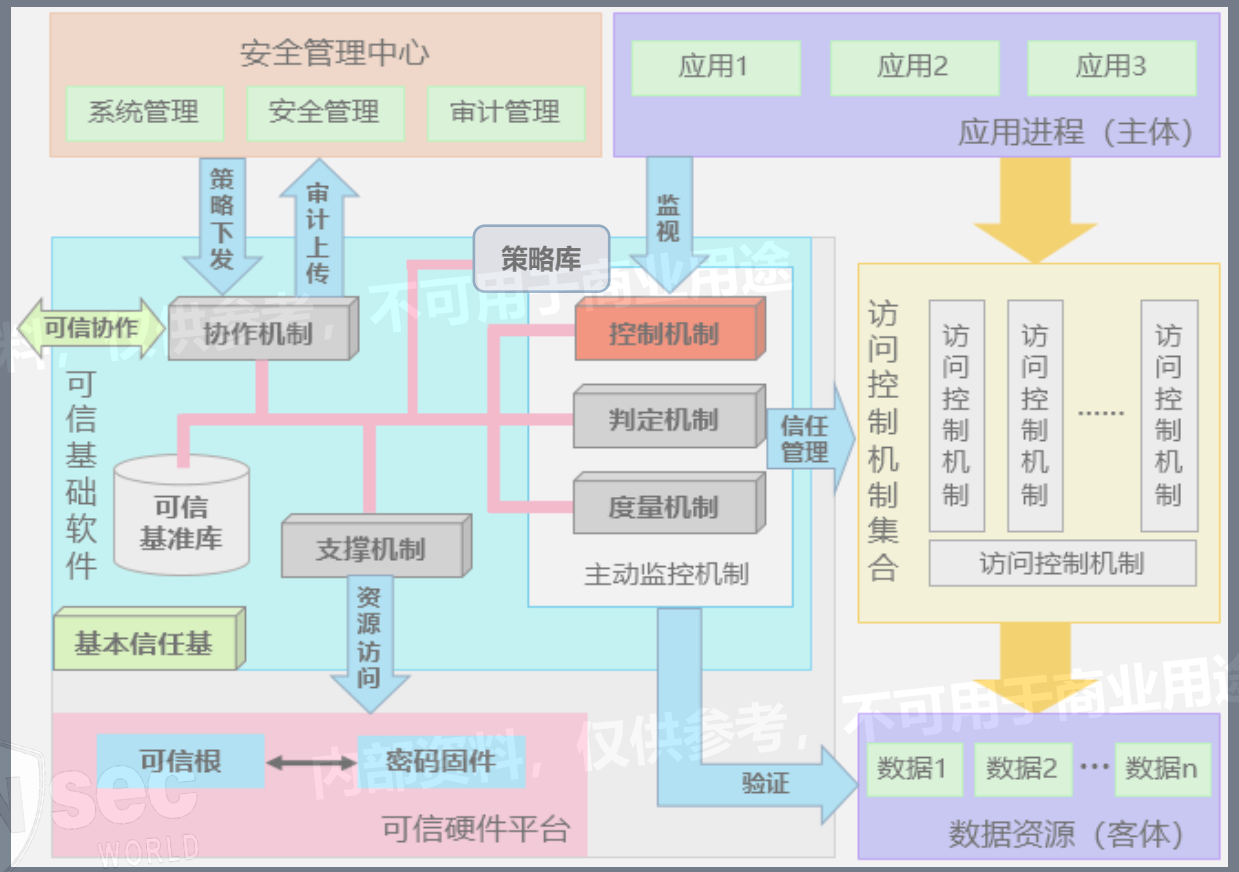
“安全办公室” “警卫室” “安全快递”



“保卫部” “保密室” “监控室”

4、“四要素”可信动态访问控制

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）进行动态可信度量、识别和控制，纠正了传统无计算环境要素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”全程管控 技管并重

按照网络安全法、密码法、等级保护制度、关键信息基础设施保护制度的要求，全程治理，确保体系结构、资源配置、操作行为、数据存储、策略管理可信。

6、“六不”防护效果

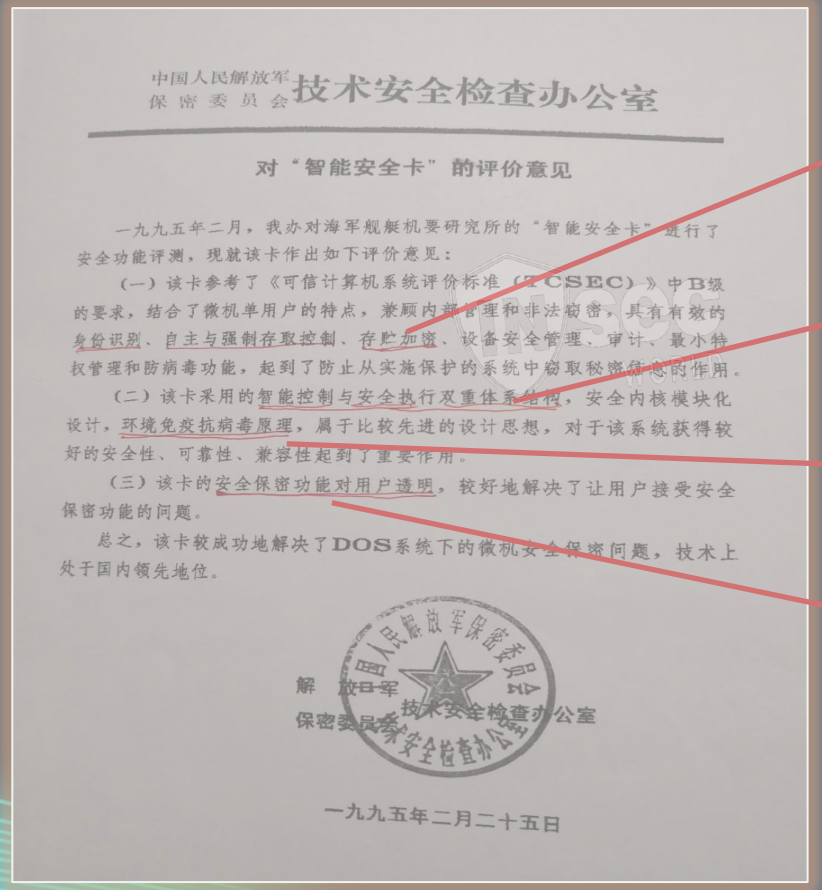
“WannaCry”、“Mirai”、“黑暗力量”、“震网”、“火焰”、“心脏滴血”等不查杀而自灭

2 PART

构建等保2.0与可信计算3.0新型产业空间

1、开创可信计算3.0时代

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破密，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

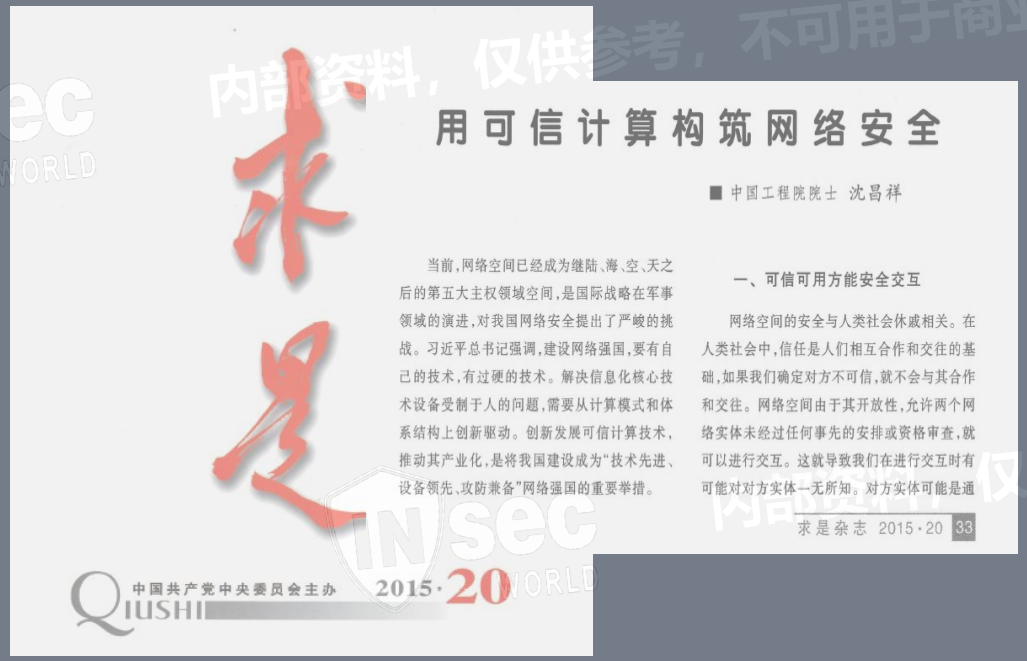
一九九五年二月二十五日

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



◆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

世界可信计算演进

	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

TPM受侧信道攻击
危及全球十几亿节点

容错组织

TCSEC → TCG

中国可信
计算创新

2、抢占核心技术制高点 摆脱受制于人

《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。

近期宣扬的零信任架构，缺少科学原理支撑，网络无边界不符合网络空间主权原则，基于身份认证的动态访问控制在国标17859早就规定，传统的调用功能模块组合难成为安全保障科学架构，也不符合我国法律、战略和制度要求推广安全可信的网络产品和服务的规定。一定要科学严谨分析研究，坚持自主创新，不能盲目跟班。

完备的可信计算3.0产品链，将形成巨大的新型产业空间

具备可信计算功能的国产CPU

嵌入式可信芯片及可信根

具备可信计算3.0技术的设备

2020年10月28日，国家等级保护2.0与可信计算3.0攻关示范基地成立揭牌

3 PART

筑牢关键信息基础设施网络安全防线

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。**

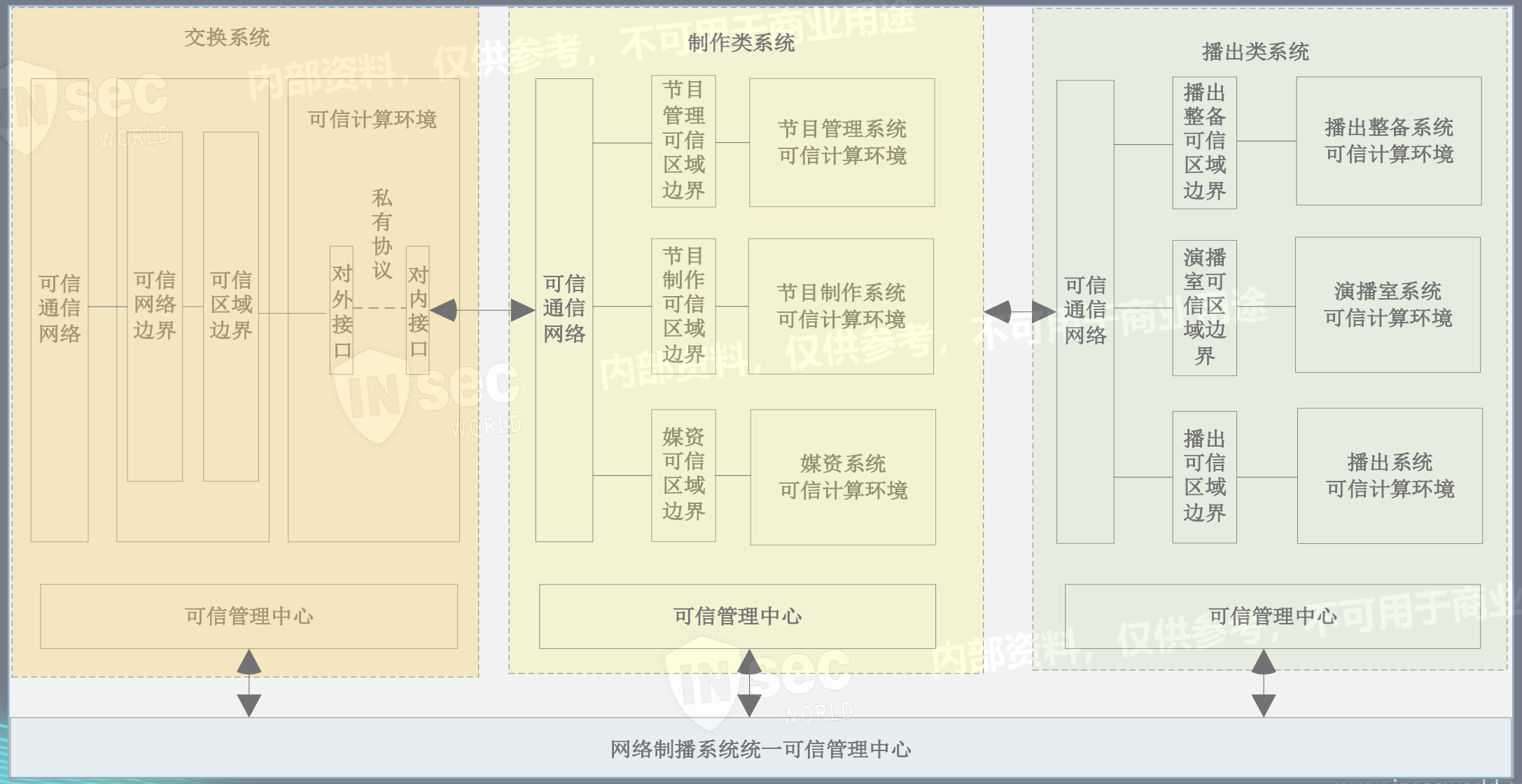
可信宿主	TCM	TPCM	检验软件	可信软件基（TSB）		
	静态可信验证基础软件可信			建链检验 应用程序可信	动态度量 执行环境	实时感知 关联态势
	BIOS	引导OS，装载系统		应用加载	应用执行	所有执行
	一级			二级	三级	四级

典型示范

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。**

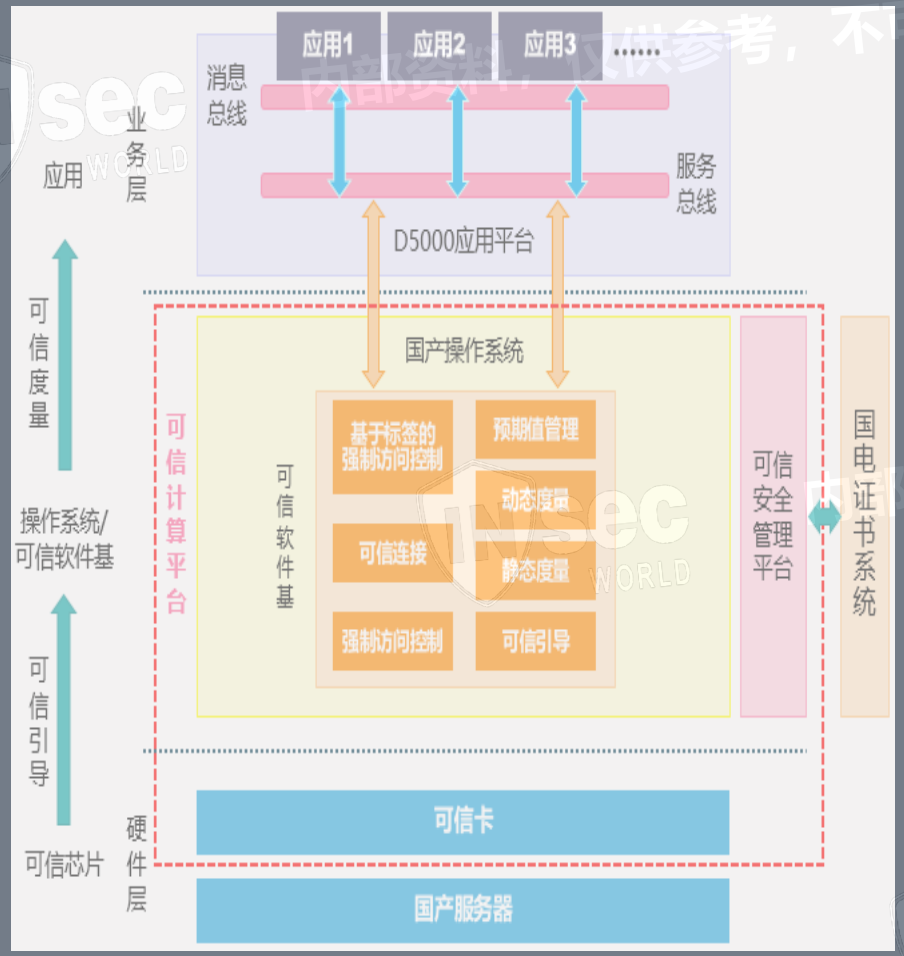
中央电视台电视节目生产、存储、编排和播出流程可信环境建设示意图



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几十个省级以上调度控制中心、上千套地级以上电网调度控制系统全覆盖，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

软硬件全国产化

- 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

谢　谢！