

信息安全技术 发展动态分析及公司介绍

主讲人：何长龙 博士
吉大正元信息技术股份有限公司 副总裁
二零零九年五月十八日

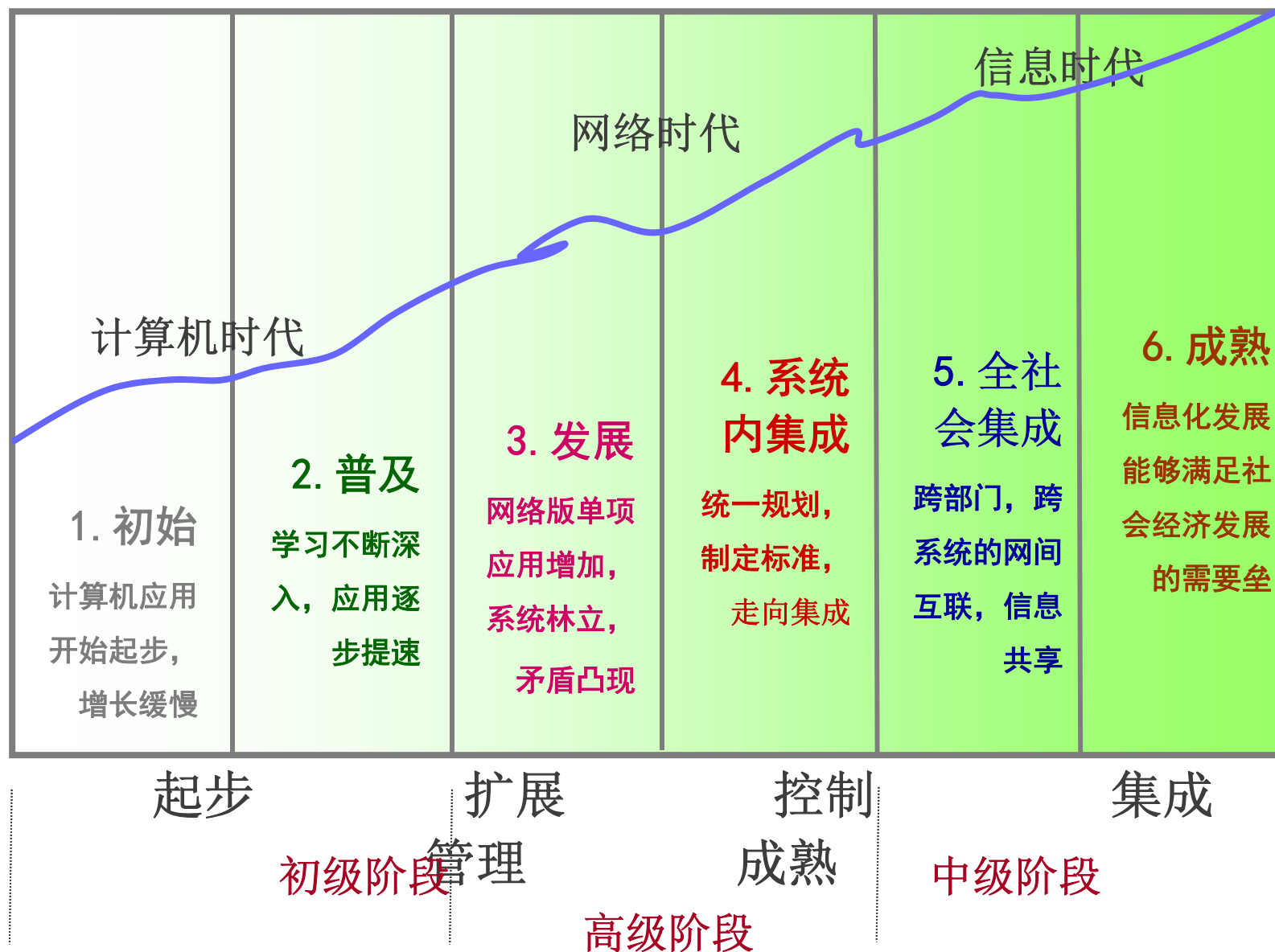


信息安全技术发展动态分析

主讲人：何长龙 博士
吉大正元信息技术股份有限公司 副总裁
二零零九年五月十八日



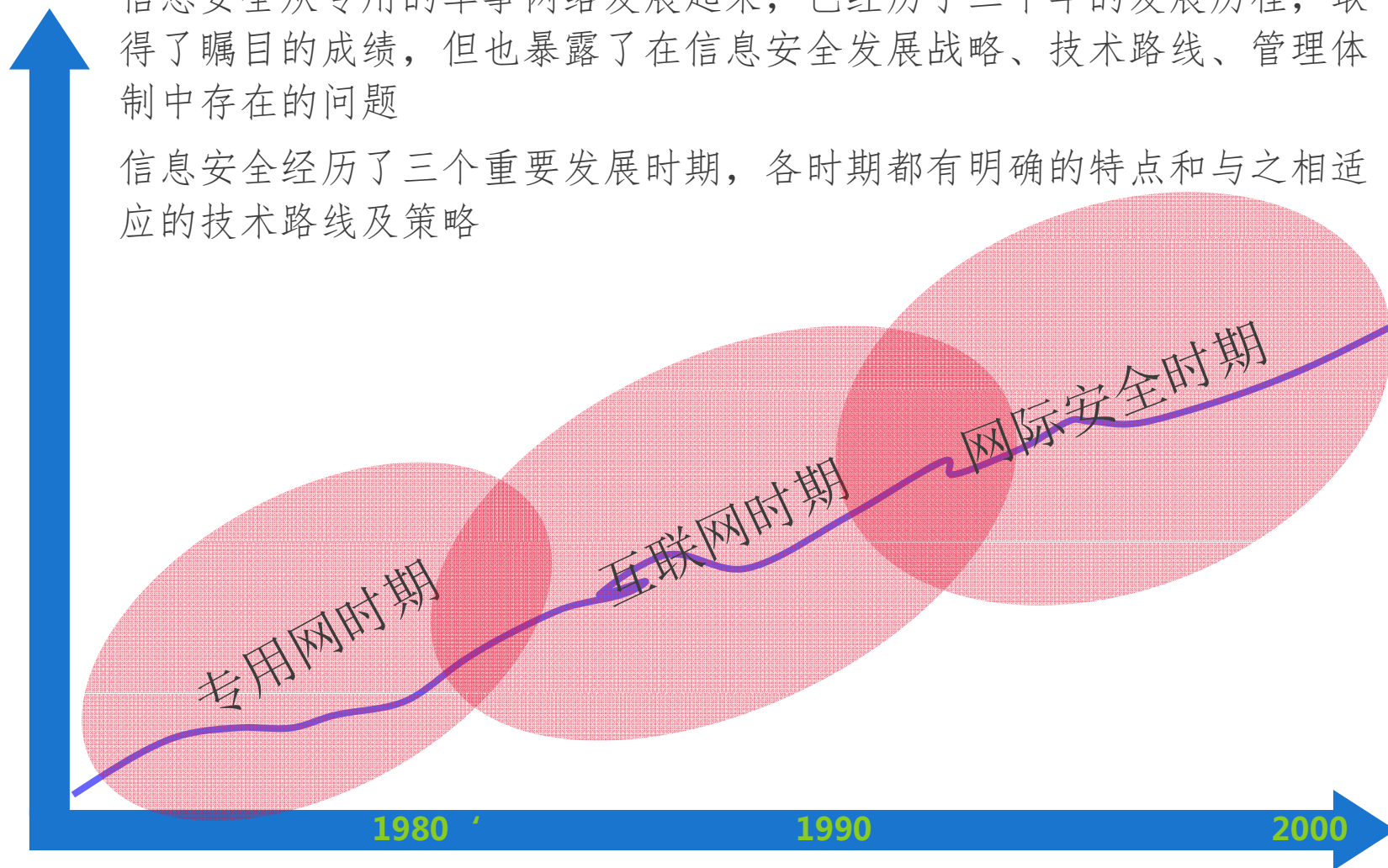
理查德·诺兰信息化阶段论



信息安全的发展阶段

信息安全从专用的军事网络发展起来，已经历了二十年的发展历程，取得了瞩目的成绩，但也暴露了在信息安全发展战略、技术路线、管理体制中存在的问题

信息安全经历了三个重要发展时期，各时期都有明确的特点和与之相适应的技术路线及策略



用网时期

由于专用网(计算机网)是封闭网，因此以等级划分、强制保护为主要策略。计算机网的通过节点打通(开放) 各终端，第一次实现计算机终端之间的交换

1981-1985年美国国防部的橘皮书（可信计算机系统评测标准）为代表，在交换网络中将人员划分为授权等级、将数据划分为秘密等级，将传统的单级管理模式发展为新型的多级控制的管理模式

80年代末，专用网管理模式在中国军事网络中得到实现和应用

专用网时期

联网时期

由于互联网是开放网，打通(开放)了网间关系，也打通了各用户之间的关系，第一次实现了用户到用户的个人化通信

这个时期的主要政策以1997年美国总统令PDD63为代表，提出以脆弱性分析为主，依靠全体网民的安全意识，实行自我把握的assurance策略——“深层次防御战略”。克林顿的assurance(自主保障)策略，打破了过去(军事的)强制性保障策略，提出了(网民的)自主性保障策略，以适应互联互通的个体化通信体制，这是观念上的一次历史性进步



专用网时期

互联网时期

联网时期的波折

1998年美国国家安全局制定信息保障技术框架（IATF）

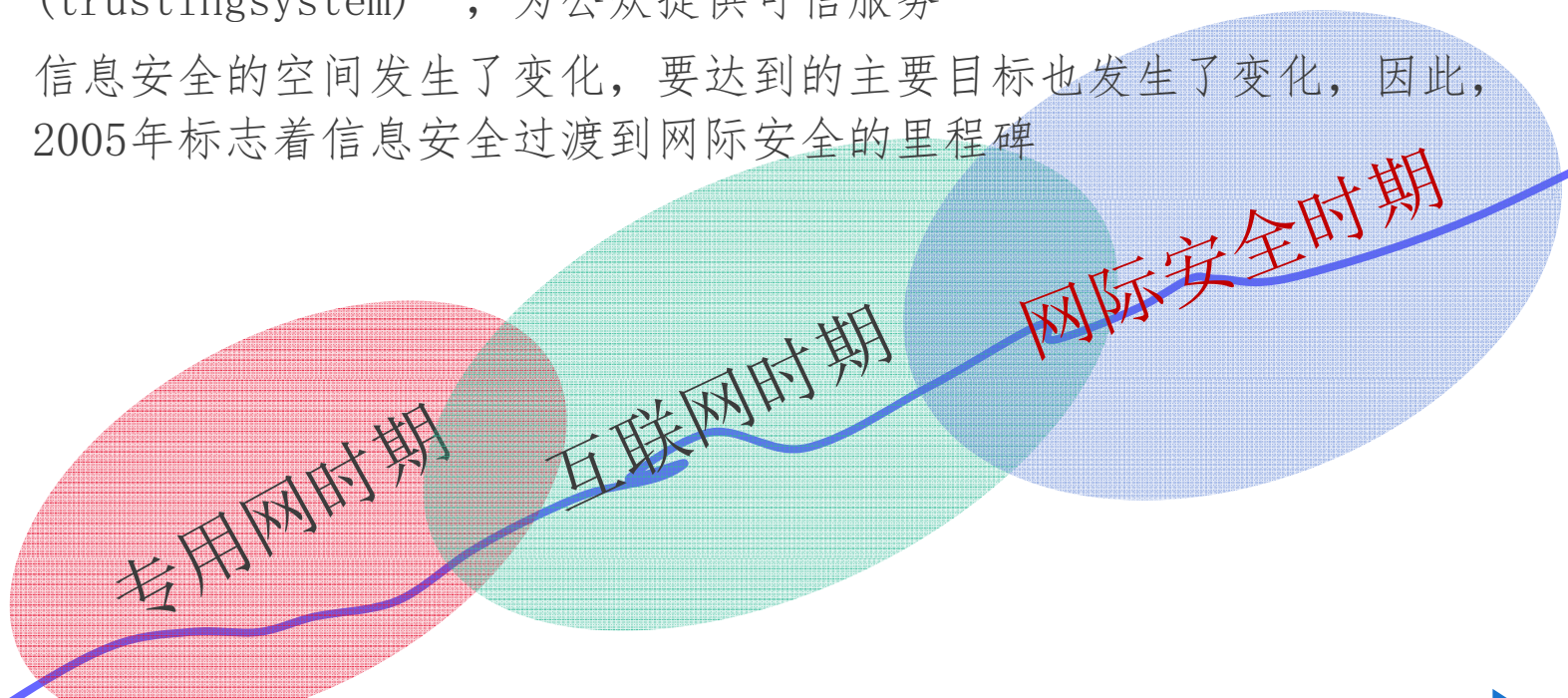
三保卫、一支撑				
保卫网络基础设施	保卫边界和外部连接	保卫局域计算环境	支撑基础设施	
无线安全 WWW安全	Firewalls	Operating Systems	KMI/PKI	Detect and Respond
	VPNs	Biometrics	PKI Protection Class 4 PKI Directory	IDS
	Peripheral Sharing Switch	Single Level Web		
	Remote Access	Tokens		
	Multiple Domain Solutions	Mobile Code		
	Mobile Code	Secure Messaging		

众网时期（网际安全时期）

信息系统已不是单纯的信息系统或网络系统，它与周围的社会结合起来构成了新的空间，这就是网际空间(cyber space)

2005年美国总统信息技术顾问委员会(PITAC)的《网际安全—优先项目危机》报告提出，网际安全的主要任务是“在危险的世界构建可信系统(trustingsystem)”，为公众提供可信服务

信息安全的空间发生了变化，要达到的主要目标也发生了变化，因此，2005年标志着信息安全过渡到网际安全的里程碑



专用网时期

互联网时期

网际安全时期

实际安全（信息安全）的含义



客户



财务



人



产品



电子邮件



文件

网际空间由相互连接而成的计算机世界和集聚在它周围的社会构成，信

网际安全——优先项目危机》

主要任务

构建可信系统，建立可信的网络秩序，为公众提供可信服务，从被动防御为主的安全转到主动管理为主的安全

主要课题

规模化认证技术是首要课题，从以脆弱性分析为主转变到以真实性判别为主

主要原则

遵循“互相怀疑”的原则。从“出于好意”的信息安全观转变到主体鉴别为主的新的网际安全观，这需要将过去信息安全理论从基于客体的“相信逻辑”提高到基于主体的“可信逻辑”。

主要方向

不局限在信息系统本身，而要包括与之相连的所有空间，如通信协议(防止非法接入)、软件工程(代码认证)、可信交易(票据认证)、网络管理(证明系统的建立)等与重要国家基

信息安全技术策略发展趋势

边缘防控向内核防控迁移

重视防外向内外兼施推进

防控对策由底层向上层过渡并集成联动

基于威胁特征向基于威胁行为复合防范转变

静态防御向动态防御发展

向跨级和跨域的纵深防御层次发展

信息安全技术策略发展趋势

边缘防控为主向内核防控为主迁移

- 可信计算就是将信息安全从源头、从行为、从体系抓起，力求使实体安全的后果是可以预期的
- 基于硬件的信任根，基于密码的身份认证，基于标签的强制访问，基于对执行代码一致性验证，基于安全模型的角色管理机制，重视系统的最小优化配置和信息安全使用的严格管理，实施系统默认即拒绝的策略和对异常行为部件先隔离后检测再放行等
- 可信计算内核是基于硬件的可信计算模块（TPM），它是可信变量与验证的基准点，实现加密、签名认证和完整性度量，配套的还包括可信计算规范（TCP），可信计算软件协议栈（TSS），可信计算架构（TCF）
- 正在成为产品的有可信计算操作系统、可信的计算终端、可信服务器、可信移动平台、可信网络接入、可信的访问控制，并将逐步向可信网络延伸

信息安全技术策略发展趋势

重视防外向内外兼施推进

➤ 内部信息安全事件的迅速增加，在防外的同时，加强信息安全的内控机制就成为关注的焦点

➤ 超过 85%的安全威胁来自企业内部

➤ 有16%来自内部未授权的存取

➤ 有14%专利信息被窃取

➤ 有 12%内部人员的财务欺骗

➤ 有 11%资料或网络的破坏

➤ 审计功能由“事后”向“事中”前移，与监控预警机制相结合。对审计信息进行保护和加固，使其具有法律的证据性（如适应国家《电子签名法》的条款）

➤ 制约和控制内部安全威胁的强审计工具迅速兴起，包括网络级审计、数据库级

信息安全技术策略发展趋势

防控对策由底层向上层过渡并集成联动

- 信息安全防控对策由网络层向应用层推进
- 信息安全防控从安全要素、系统要素和网络要素进行综合集成，实现对威胁信息的共享和安全功能的协同联动，以提升对威胁定位和定性的准确度，降低虚警率和漏警率
- 由于在多个层次上采用综合治理，这将会提升安全治理的效果
- UTM、SOC和应用层安全对策等技术产品都体现了综合集成安全治理的效果，它将有很大的发展空间

信息安全技术策略发展趋势

基于威胁特征向基于威胁行为复合防范转变

- 新型威胁及其变种的快速演变，对其鉴别将缺少足够的先验信息，单纯靠其特征鉴别已经是不完备的，因此基于威胁行为的防范工具将更有效地鉴别和对付病毒、蠕虫、木马等各种新型的恶意代码，势在必行。
- 对于内部作案者的非常规行为的鉴别与治理将提升内部防范的有效性，基于行为的安全防范工具和产品正在兴起，前景看好

信息安全技术策略发展趋势

静态防御向动态防御发展

- 没有攻不破的防线，保证系统作业允许的可持续性（BCP）要求，使系统资源的损失低于系统资源可承受的能力，使系统服务中断时间小于系统中断风险最小可承受的能力
- 完整的动态防御流程体系应包括预警、防护、检测、响应、恢复和快速取证的全过程（WPDRRA），动态防御流程的协调和优化是动态防御全局和有效的关注点，其中包括各安全机制和安全产品的协同联动，虚拟信息资产的重新部署，网络动态拓扑结果的调整，以达到将安全风险降低到可承受的水平。该安全理念和技术已有长足的进展，还有更深化的发展空间

信息安全技术策略发展趋势

向跨级和跨域的纵深防御层次发展

- ▶从信息化应用工程的局域网到园区网、城域网、省际网、全国网,从信息系统的涉密内网、敏感的专网、外网到开放的互联网,复杂巨型系统的信息安全域的划分、管理和信息跨安全域的流动成为尖锐问题
- ▶安全等级划分中,在同一等级内如何划分不同的安全域,信息在不同安全域间是要流动的,为了保证信息跨域的安全和有效交换与共享,如何制订跨域交换的控制机制和策略
- ▶科学划分信息安全域,制订跨域信息安全交换安全策略,选择信息安全边界控制机制,正确部署边界信息安全产品(FW、NG、GAP、VPN、VLAN等),以达到即有利于信息快速流动和业务有效运转,网络应用业务流畅与高效,又保障信息与应用的安全,在该领域内各类技术和产品发展很快,但真正要做到即有效又安全,即简单又可信,还要进一步深入探索和加快推进,以全面满足信息安全纵深防御的要求

信息安全技术发展状况—基础类

机密性、完整性、
不可否认性算法

算法研究是基础研究，属于数学范畴，近年来没有革命性的新算法广泛应用。随着计算能力的不断增强，机密性、完整性不可否认性算法等方面研究需要进一步加强

特征识别模式匹
配技术

为有效避免垃圾信息、病毒以及其他有害信息通过网络扩展，必须进一步研究特征识别以及模式匹配等技术。当前对网址、关键字过滤有一定进展，在图片、影片、声音等方面有待进一步研究和应用

安全芯片、操作
系统、设备技术

安全相关的芯片、器件、软件、操作系统、专用设备等都是网络与信息安全的基础。当前上述技术在国际上相对成熟，除非有重大突破，当前重点在于综合应用

安全体系理论

安全体系结构理论主要研究如何利用形式化的数

信息安全技术发展状况—应用类

认证鉴权技术

通过一定的协议流程和算法验证持有特定密钥的用户是否是所声称的特定用户，拥有什么样的权限。近年来，鉴别密钥有所发展，当前ITU等组织正在研究生物特征鉴别

海量信息处理

当前网络随着通信需求的增加以及光通信等技术的飞速发展，在合法监听、内容检测、防范入侵和攻击中，需要实时或者短时间内处理大量信息。因此海量信息处理，包括深度协议感知、线速过滤、模式匹配、海量存储等技术都在研究中，并且是近期内的重要研究方向安全

数字水印等

随需求的不断出现，新的安全技术将被研究和应用

信息安全技术发展状况—综合类

可靠性技术

通过器件、设备、协议以及网络组织使网络/应用系统能够持续不间断提供服务。当前传统电信网相关的可靠性普遍认可，可靠性研究比较成熟；基于IP网络的可靠性还有待提高，因此研究还在继续，同时新的研究成果还正在应用到IP网络特别是NGN承载网别

溯源技术

通过技术手段，将内容、网络行为以及应用行为等追溯到该行为发起者。IP网络以及应用服务溯源技术正在进展中。随着各国对网络基础设施依赖性的增加，溯源技术将和认证鉴权技术、安全通信架构等结合在一起保障安全

信息对抗技术

随着社会对网络基础设施依赖程度的增加，信息对抗成为国与国对抗的重要内容。当前信息对抗

信息安全技术发展状况—综合类

应急通信

主要是在灾年以及战争等通信设施瘫痪的情况下如何保证必要通信能力持续提供的行为。传统电信网应急通信研究比较成熟，互联网/IP网以及基于IP网新业务和网络的应急通信还在研究中

风险评估

信息系统安全风险评估在ISO等组织研究相对成熟，对网络系统的评估方面还有待进一步研究和应用

反垃圾信息

反垃圾信息实际上并不是一种具体的技术，而是模式识别、管理、架构方面的综合应用。当前国际国内都非常重视反垃圾信息，正在热点研究中

体系架构

合理有效的架构能够综合各种技术，在网络与信息系统中提供合法监听点、传输传播控制点、为通信双方信任体系，用户隐私保护等。架构、框架等综合应用是当前以及未来网络与信息安全研

信息安全的核心技术

➤从技术层次上讲，信息安全的核心技术是：**认证和授权**

➤认证技术主要用于建立网络世界秩序，授权（监管）技术则用于对网络世界的管理和控制

➤认证技术的重要性在于：它可以解决网络环境下复杂的身份识别和定位问题；由于认证技术的基础是密码技术，它将把网络攻击的技术门槛从一般计算机技术提升到专业密码分析，黑客将望尘莫及

信息安全产品的发展

安全产品

安全硬件

令牌

智能卡

生物识别

防火墙/VPN

安全内容管理

入侵检测

入侵防御

统一威胁管理

其它

安全软件

身份管理与
访问控制

安全性与
漏洞管理

安全内容
管理

威胁管理

PKI

事件管理

防病毒

软防火墙

高级认证

漏洞管理

WEB流过滤

入侵检测软件

单点登录

安全策略
与执行

消息安全

入侵防御软件

遗留系统认证

目录服务

安全服务

规划

实施

运维

培训

国信息安全产品发展趋势

产品标准化

产品产业化

管理一体化

服务专业化

产品国产化

专用网时期

互联网时期

网际安全时期

我国信息安全未来的关注：战略层面

■ 《国家中长期科学和技术发展规划纲要》

◆将“面向核心应用的信息安全”列为优先发展主题之一，明确提出“以发展高可信网络为重点，开发网络信息安全技术及相关产品，建立信息安全技术保障体系，具备防范各种信息安全突发事件的技术能力”

■ 《2006-2020年国家信息化发展战略》

◆提出全面加强国家信息安全保障体系、增强国家信息安全保障能力的战略目标，战略可概括为信息安全保障六项工作（之二建设以密码为基础的网络信任体系）

吉大正元信息技术股份有限公司

公司介绍

本情况

成立时间： 1999年2月

注册资本： 7500万元

公司资产： 近3亿元

员工总数： 380余人

公司定位：

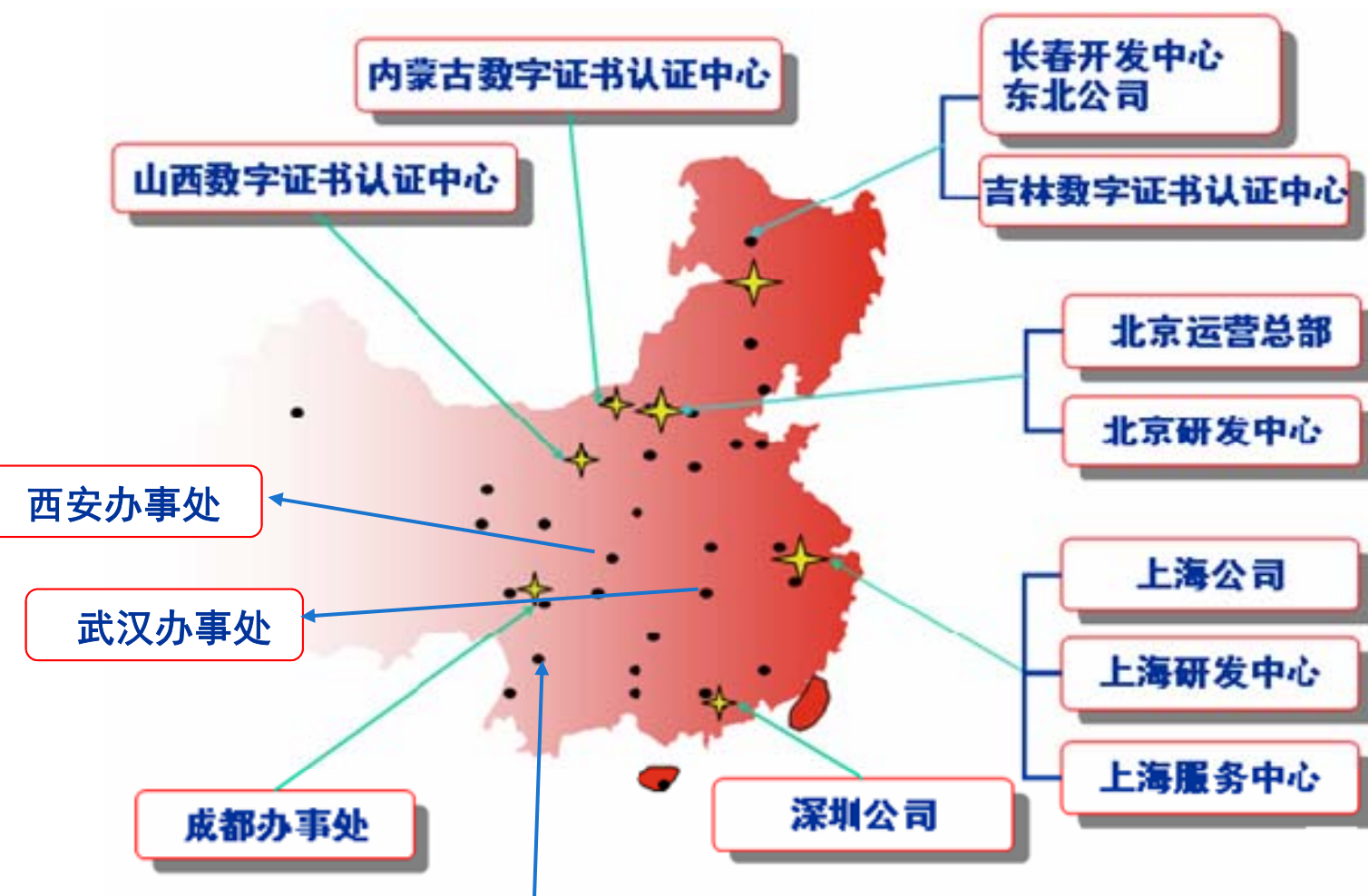
- ◆国内领先的信息安全产品、服务、解决方案提供商
- ◆基于PKI/PMI技术解决认证、授权、管理、内容保护等应用安全问题

公司资质：

- ◆48项自主知识产权
- ◆76项资质证书

国家科研项目、标准建设的主要参与者

织结构



司资质

- 首批国家商用密码产品定点生产单位
- 首批国家商用密码产品销售许可单位
- 计算机信息系统一级集成资质
- 涉及国家秘密的计算机信息系统集成资质证书（甲级）
- 涉及国家秘密的计算机信息系统软件单项资质
- 解放军信息安全评测中心军用产品认证
- 公安部信息安全产品销售许可证
- 国家信息安全测评中心安全产品认证
- 国家信息安全标准技术委员会成员
- 国家863计划成果产业化基地
- 国家火炬计划软件产业基地骨干企业
- 国家规划布局内重点软件企业

上海市重点高新技术企业

家贡献

国家标准

- ◆ WG4组: 《数字证书格式》、《证书认证策略与规范CP/CPS》、《证书认证接口规范》(召集单位)
- ◆ WG3组: 《证书认证系统检测规范》、《密钥管理系统检测规范》(召集单位)

行业标准

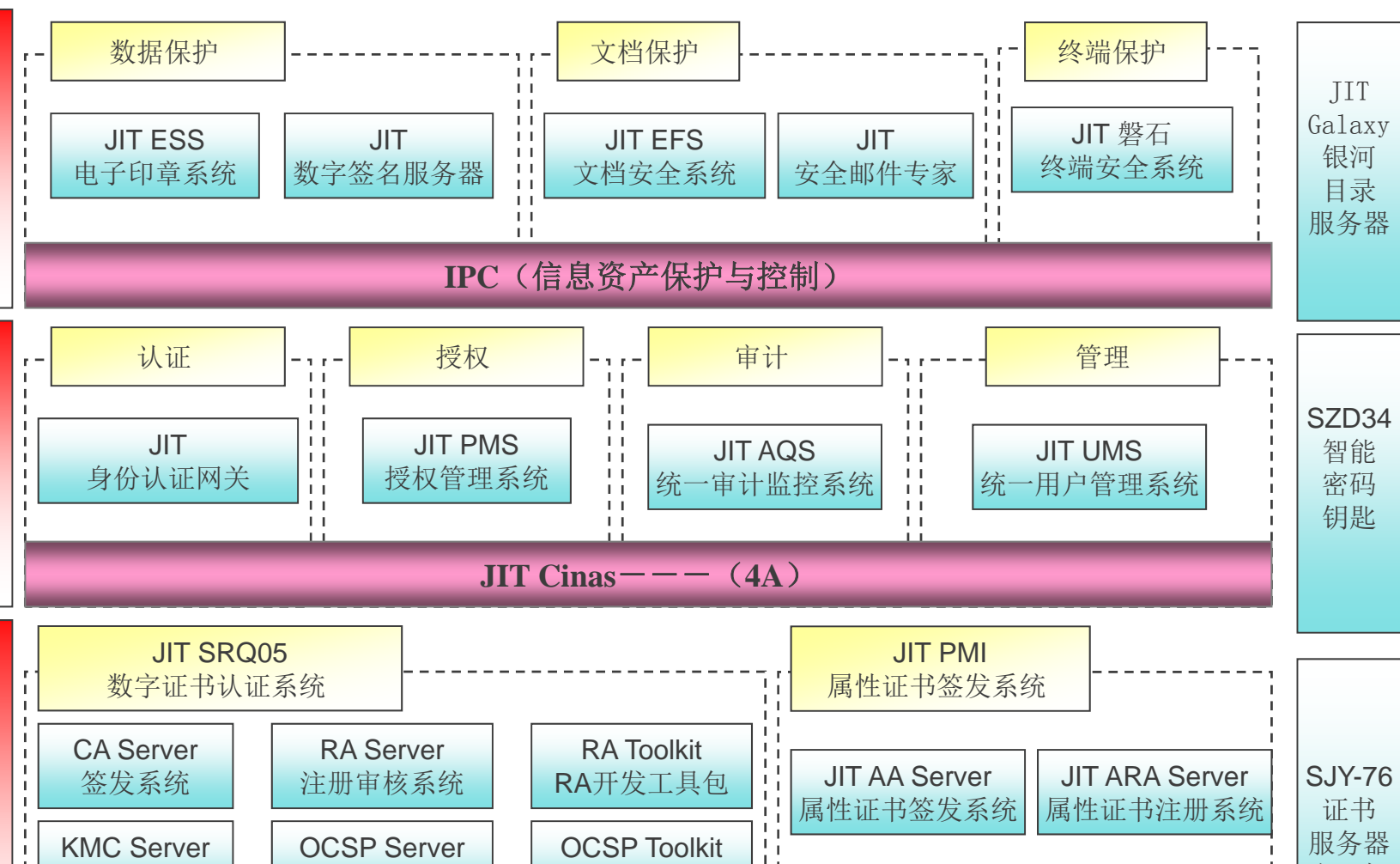
- ◆ 公安行业、监察部、军工行业、金融等行业标准

国家项目 (共计21项)

- ◆ 4项国家工信部 (信产部) 项目
 - 《吉大正元电子证书JIT-CA及其应用系统》
 - 《面向电子签名与认证授权的安全应用支撑平台》
 - 《基于智能卡的数字证书系统》
 - 《网络安全隔离与信息交换设备与系统》
- ◆ 5项国家发改委重点项目、6项国家科技部项目、2项863计划、2项火炬计划项目、2项中小企业创新基金

2005年获国家发改委批示组建“信息安全共性技术国家工程研究中心”(国家

品家族



产品设计理念

安全为应用服务，安全为管理服务

安全性与可用性、易用性结合

一个平台、四个统一功能、一套资产保护

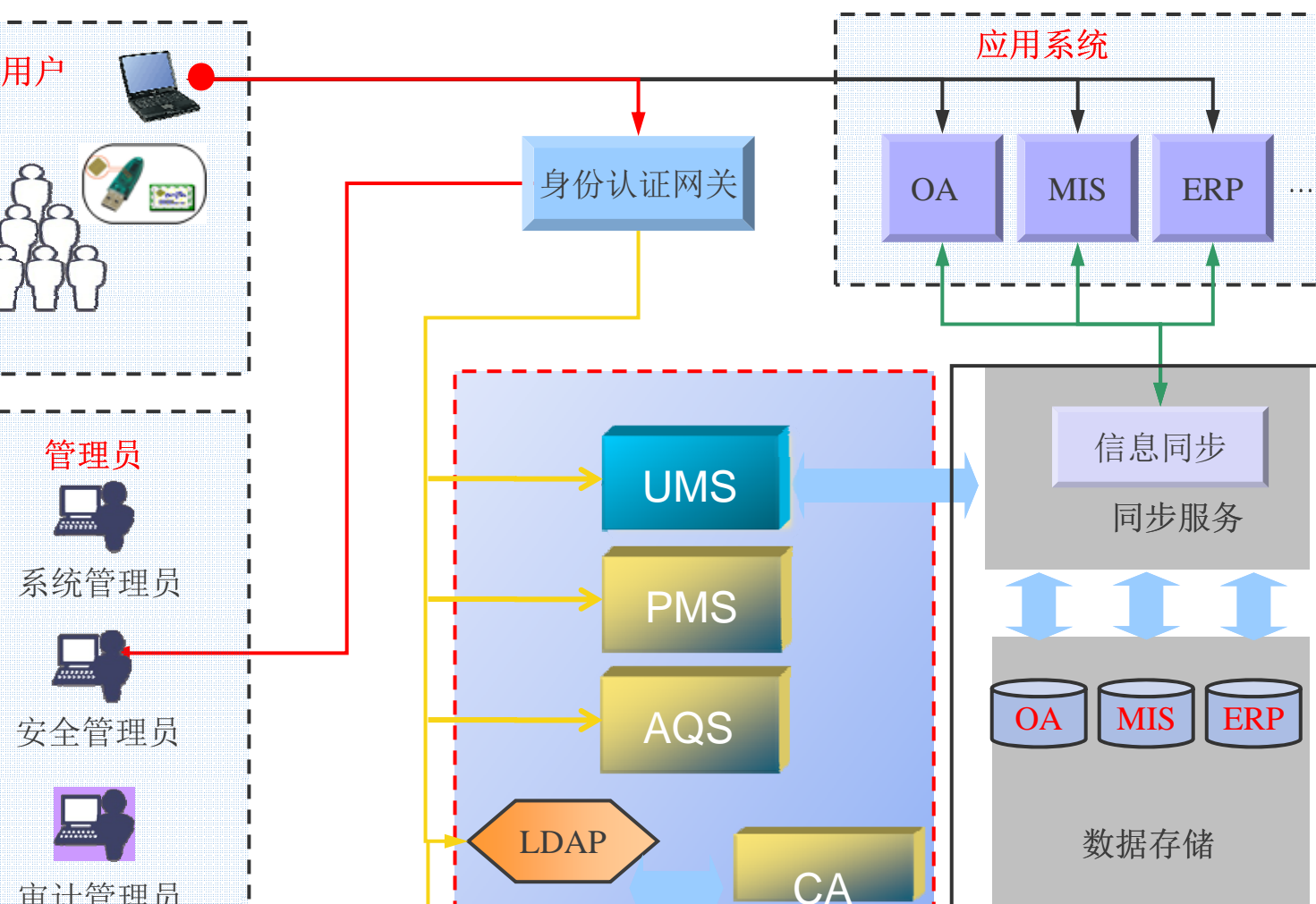
一个平台：应用安全支撑平台

四个统一功能：统一认证、统一授权、审计、管理

一套资产保护：终端、文档、数据

保护原有用户投资、尽量避免调整应用——业务无关性

产品介绍—应用场景



解决方案收益分析



品荣誉

《SRQ05电子证书认证系统》

- ◆ 完全自主知识产权
- ◆ 第一个通过国家级鉴定
- ◆ 国家重点新产品
- ◆ 科技进步一等奖

《应用安全支撑平台》

- ◆ 第十届中国国际软件博览会金奖
- ◆ 2008中国十大创新软件产品



术能力

吉林大学

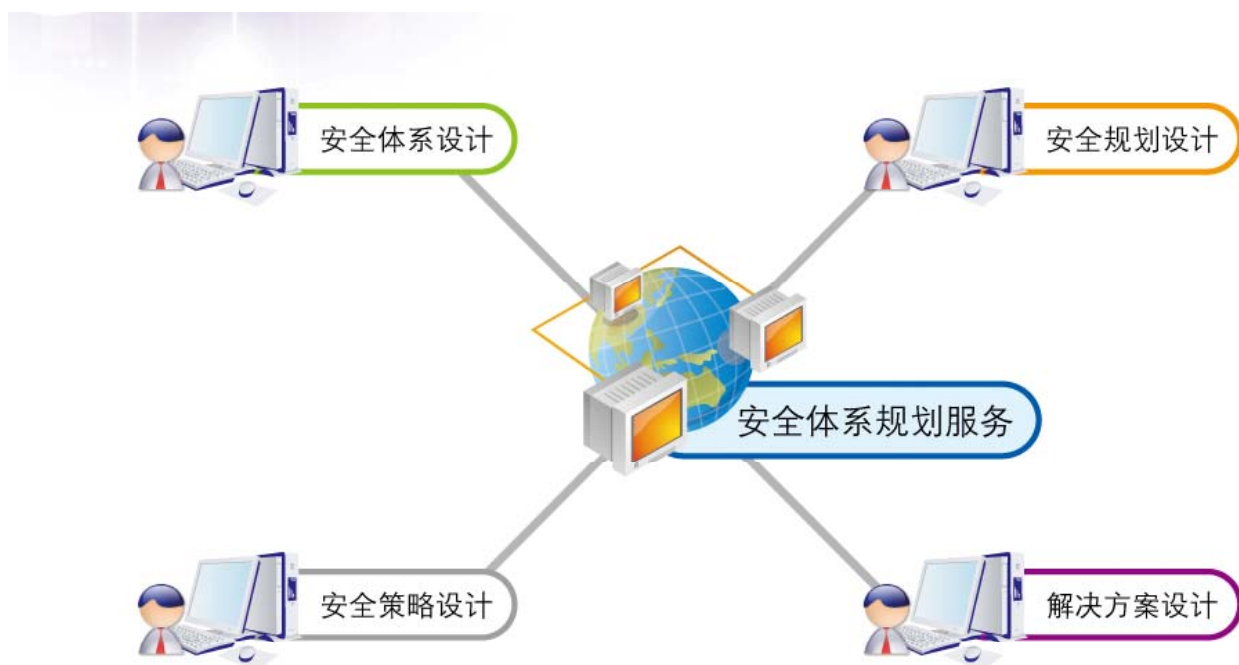
国家信息安全重点实验室

拥有近200人的专业研发队伍

结构完善的专家队伍

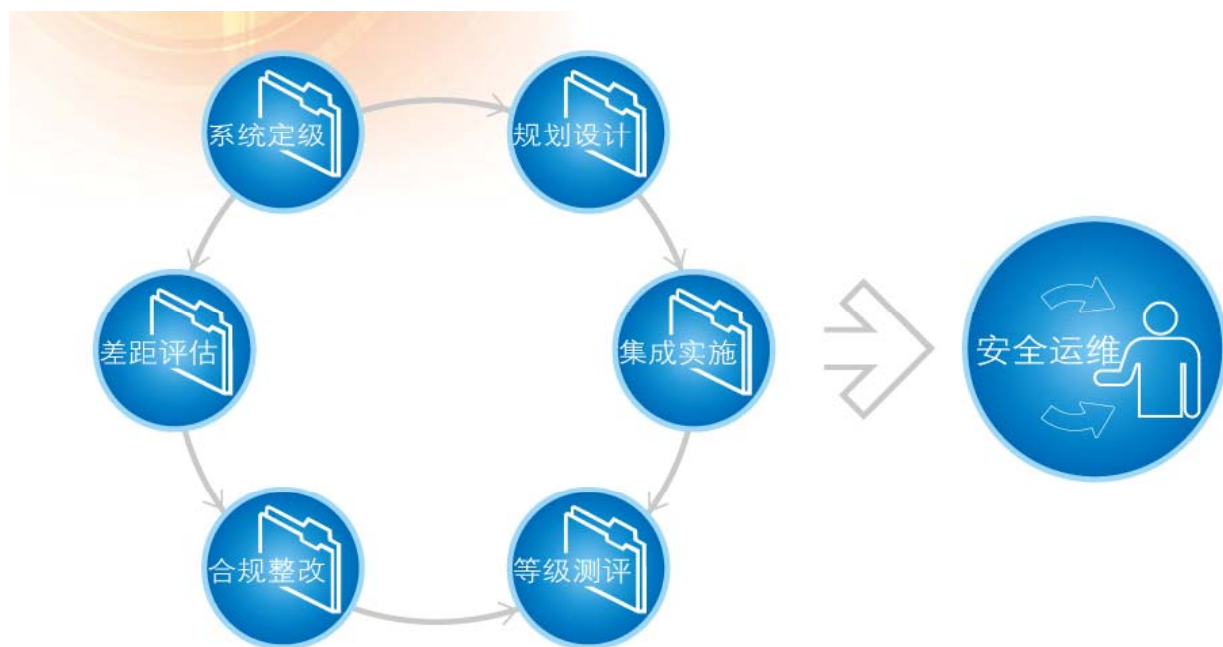
国家科研项目的积累

全服务体系-----安全体系规划



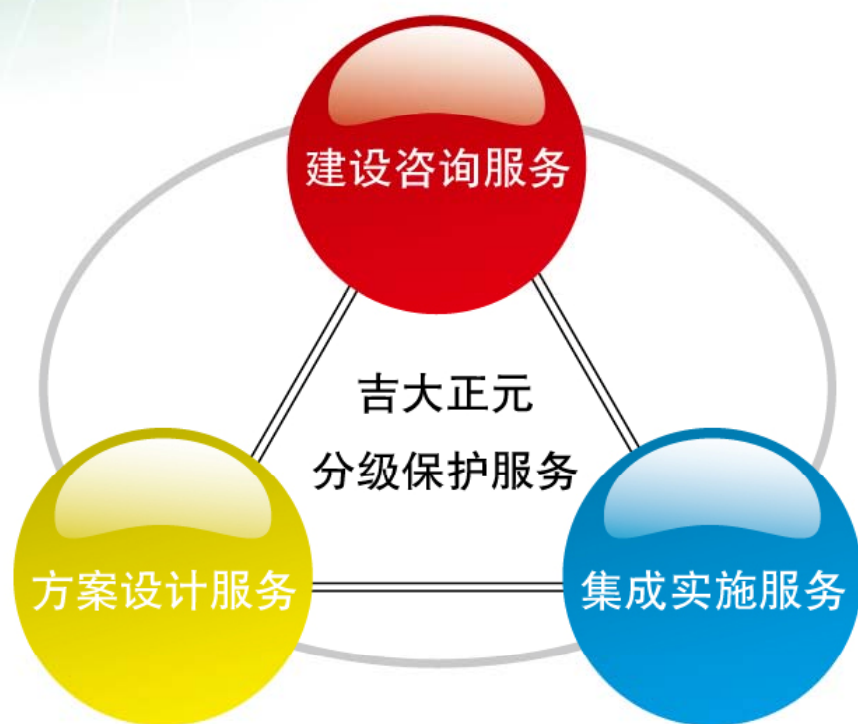
根据信息系统的安全现状，结合国家与行业政策标准要求，为客户设计整体安全体系框架、安全策略与技术解决方案、安全建设规划，满足客户在安全建设、运维、检测、评估、应急响应等方面的需求。

全服务体系-----等级保护



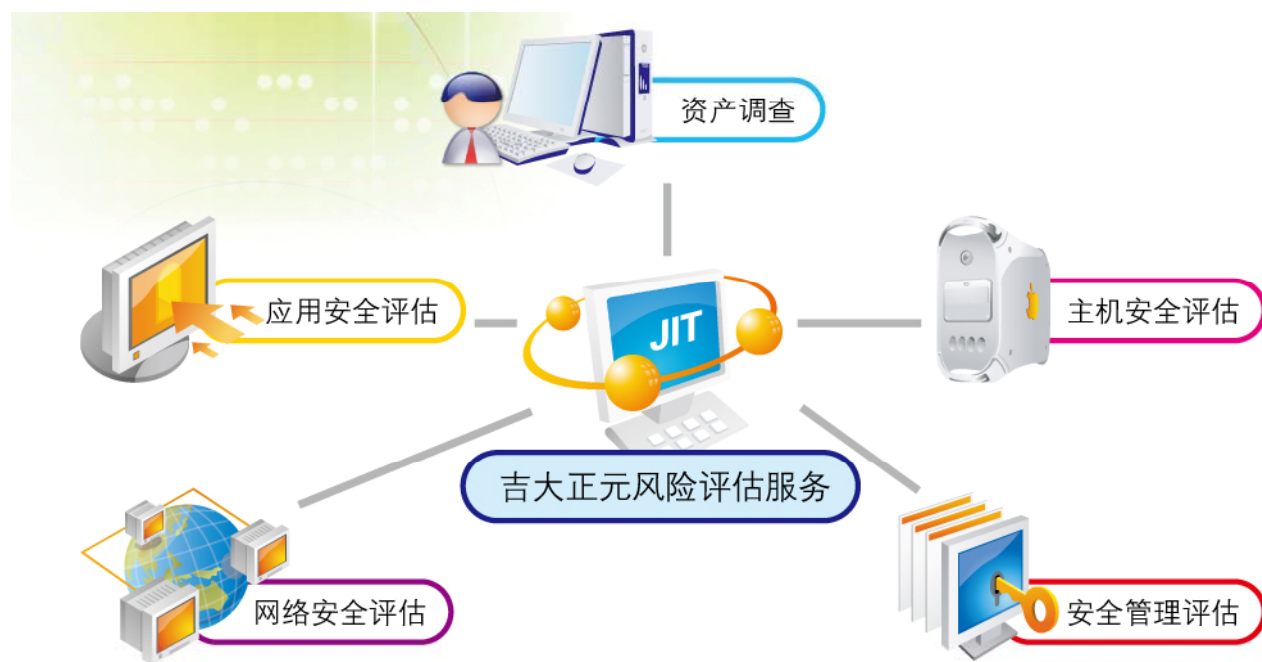
吉大正元等级保护服务是依据国家等级保护相关标准和用户安全需求，为提供系统定级、差距评估与整改、规划设计、集成实施、等级测评、安全等全生命周期的安全服务，满足国家等级保护要求。

全服务体系-----分级保护



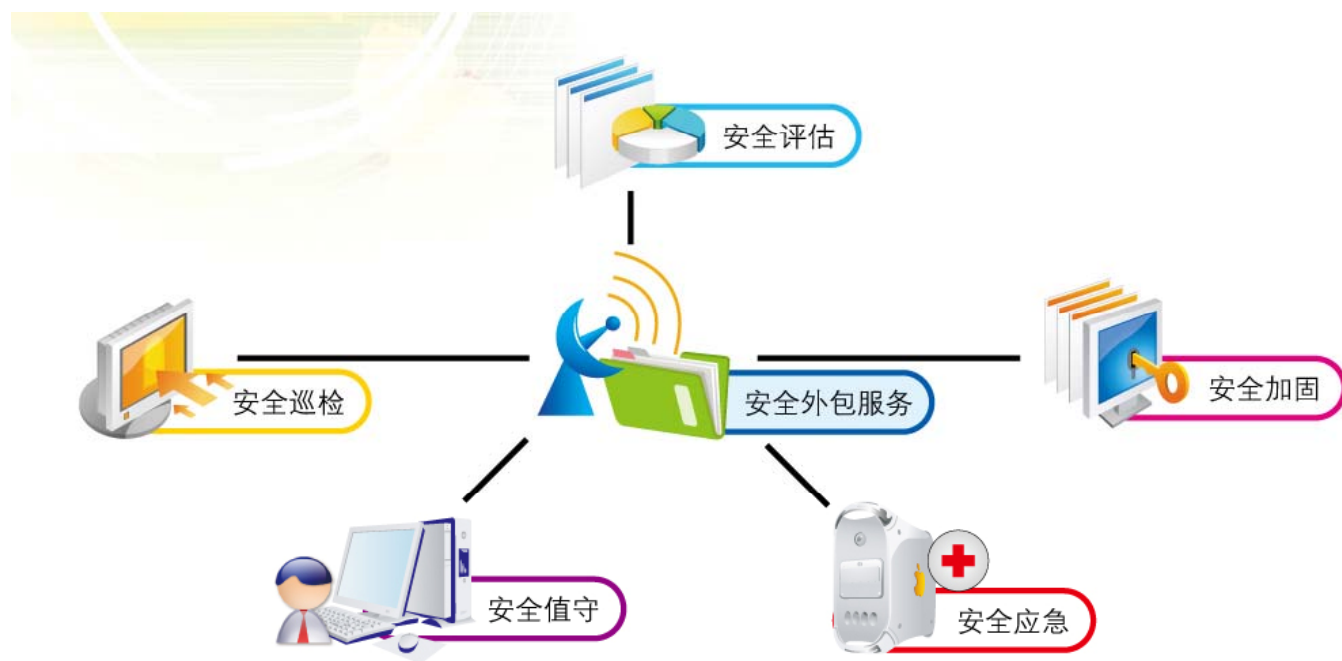
根据分级保护要求和系统安全现状，构建整体安全体系架构，提供完整生命周期内的安全体系建设咨询和整体方案设计，并完成产品安装部署、管理策

全服务体系——风险评估



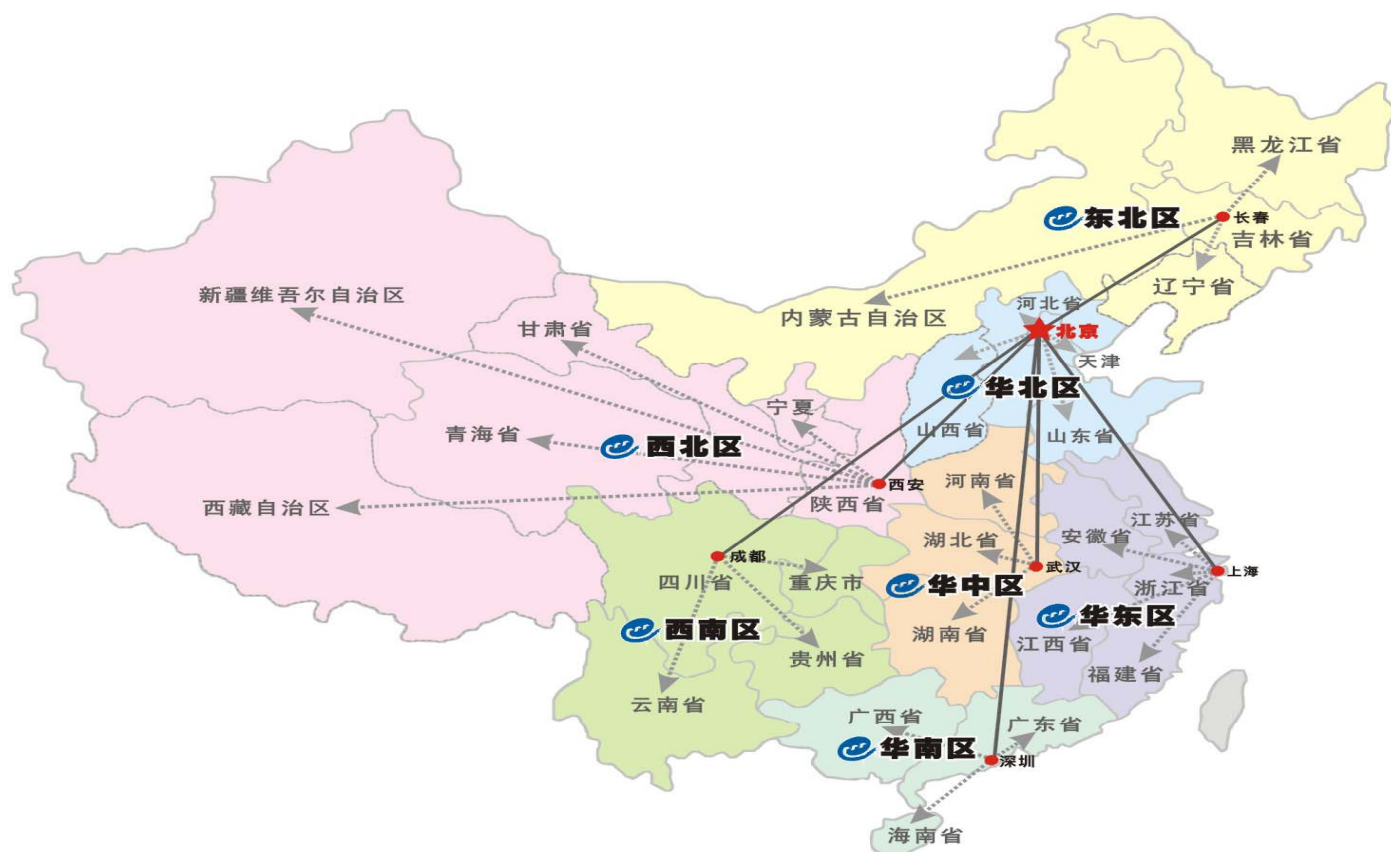
从资产评估、主机安全评估、网络安全评估、应用安全评估和安全管理评估五个方面全面分析信息系统的安全弱点及风险。

全服务体系——服务外包



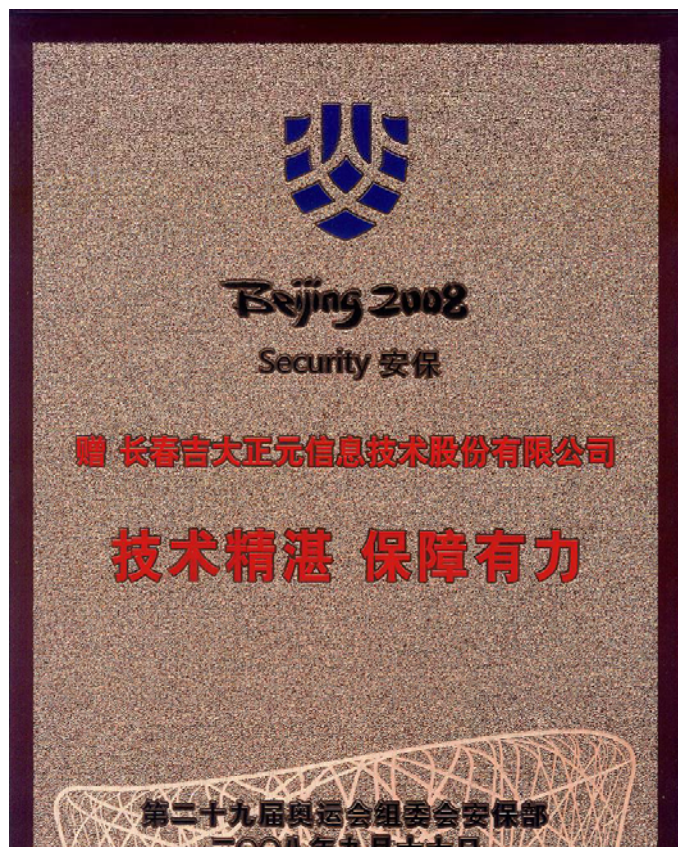
吉大正元安全服务外包基于ITIL服务管理的流程，提供了包括安全评估、安全加固、周期性安全巡检、重要时期安全值守、以及安全事件应急响应等完整的安全运维服务。

务网络



新服务荣誉

为第二十九届奥运会保驾护航，服务表现卓越



功案例（一）电子政务

- 全国人大、全国政协
- 中央纪委、中联部电子政务示范工程
- 国务院、国家发改委纵向网
- 国家工业与信息化部
- 国家财政部——金财工程（建设中，未来全国最大的部委4A体系）
- 国家公安部——金盾工程（已建成，目前全国最大的部委4A体系）
- 国家水利部——金水工程
- 国家审计署——金审工程
- 国家质监总局——金质工程
- 国家监察部、国家铁道部
- 国家交通部、国家信息中心“互联互通示范工程”
- 国家宗教事务局、国家地震局

功案例（二）电子商务

金融证券业

- ◆中国人民银行、中国金融认证中心CFCA
- ◆中国银行、招商银行、银联、光大银行等八家商业银行
- ◆上交所、深交所
- ◆人保财险、太平洋保险等

电信业

- ◆中国移动、浙江移动、北京移动、重庆移动、四川移动等
- ◆中国联通全网

功案例（三）电子军务

队级

- ◆国家军盾1号作战指挥系统
- ◆总装、总参、海军机要局等
- ◆成为军队信息化建设重要组成部分
- ◆目前军方在吉大正元设有军代表，完成军品质量体系认证

工级

- ◆中国船舶工业集团公司
- ◆中国兵器装备集团公司
- ◆航天科工集团公司
- ◆核工业集团公司
- ◆航空一集团公司
- ◆航空二集团公司
- ◆核动力研究设计院

功案例（四） 能源行业

国家电网体系：

- ◆ 国家电网集团公司总部
- ◆ 辽宁省电力公司
- ◆ 吉林省电力公司
- ◆ 黑龙江省电力公司
- ◆ 重庆电力公司
- ◆ 山西省电力公司

中国华电集团公司

国电泰州发电公司

中国国电集团公司

中国神华集团

... ..

■ 南方电网体系：

- ◆ 南方电网集团公司总部
- ◆ 南方电网超高压输电公司
- ◆ 南方电网调频调峰发电公司
- ◆ 广西省电力公司
- ◆ 贵州省电力公司
- ◆ 海南省电力公司
- ◆ 云南省电力公司

A scenic view of the Great Wall of China winding through misty mountains. The wall is visible in the foreground, leading up a hill towards a watchtower. The background features rolling mountains partially obscured by a thick layer of white mist or fog, creating a serene and atmospheric landscape.

自主 创新 服务 回报