

本文目录

- [北信源有央企背景吗？](#)
- [itp软件原理？](#)
- [信息安全保密管理的基本内容？](#)

北信源有央企背景吗？

有。

北信源（300352.SZ）11月23日在投资者互动平台表示，公司是国内终端安全管理领域的龙头企业，是国内网络与信息安全领域领先的解决方案提供商，为客户提供涵盖网络与信息安全的软件开发、运维管理以及系统集成在内的行业级、城市级体系化信息服务解决方案。公司秉承“为中国的数字化腾飞保驾护航”的企业使命，深度布局信创安全、数据安全，已累计15年实现国内终端安全管理市场占有率第一。与数字化转型紧密相连的数据安全方面，北信源的商密文档安全产品在工商银行完成60万点部署后，成为了商密的业界标杆，相继被中国联通、国电投、中粮集团等央企选用；北信源的数据防泄漏（DLP）等产品更是被中国移动、中石油和中海油等重要单位选用，公司在信创数据安全细分市场已经形成先发优势。近期数据安全类项目较多，集中于大中型国企、央企、国有单位等客户，受到广泛肯定。

itp软件原理？

ITP的核心理念可以概况为一句话：通过识别和管控企业内部有威胁的人的行为，来降低数据泄漏和其他风险。

ITP强调的是以人为核心的内部威胁防范，通过识别用户的行为和其产生的各种数据，利用人工智能和大数据等技术手段将其关联，对高风险用户的危险行为及其他用户的类似行为进行管控，从而实现危险行为的阻断并预防类似行为的发生。

识别和管控并非新兴技术，一直都是传统数据防泄漏方案的基本支撑。但ITP综合考虑了网络管控、内容感知，以及更重要的用户行为等因素，同传统DLP技术相比，更加的智能化，有着更低的误报率和更高的检出率，此为ITP技术体系的最大的特点。

原理是在内容感知技术之上(ASWG+DLP)，加入了对用户、网络和终端行为与事件的风险分析，并根据具体情况，针对性地对用户和终端行为进行培训，然后将培训结果评级调整，最后再返回给DLP的安全策略。这一过程包括了UEBA、统计学异常分析、贝叶斯统计模型、机器学习等关键技术。

信息安全保密管理的基本内容？

信息安全包括：

(1) 物理安全。物理安全主要包括环境安全，设备安全和媒体安全。处理秘密信息的系统中心房间应采取有效的技术预防措施。重要系统还应配备保安人员进行区域保护。

(2) 操作安全。操作安全性主要包括备份和恢复，病毒检测和消除以及电磁兼容性。应备份机密系统的主要设备，软件，数据，电源等，并能够在短时间内恢复系统。应当使用国家有关主管部门批准的防病毒和防病毒软件及时检测和消毒，包括服务器和客户端的病毒和防病毒软件。

(3) 信息安全。确保信息的机密性，完整性，可用性和不可否认性是信息安全的核心任务。

(4) 安全和保密管理。分类计算机信息系统的安全和保密管理包括三个方面：管理组织，管理系统和各级管理技术。建立完善的安全管理机构，建立安全保障管理人员，建立严格的安全保密管理体系，运用先进的安全保密管理技术，管理整个机密计算机信息系统。

信息安全本身涵盖范围广泛，包括如何防止商业企业机密泄露，防止年轻人浏览不良信息以及泄露个人信息。

网络环境中的信息安全系统是确保信息安全的關鍵，包括计算机安全操作系统，各种安全协议，安全机制（数字签名，消息认证，数据加密等），直到安全系统，如 UniNAC，DLP 等安全漏洞可能威胁到全球安全。

信息安全意味着信息系统（包括硬件，软件，数据，人员，物理环境及其基础设施）受到保护，不会出于意外或恶意原因，被破坏，更改，泄露，并且系统可以连续可靠地运行。信息服务不会中断，最终实现业务连续性。

信息安全规则可以分为两个层次：狭隘的安全性和一般的安全性。狭隘的安全性基于基于加密的计算机安全领域。早期的中国信息安全专业通常以此为基准，辅以计算机技术和通信网络技术。与编程有关的内容；广义信息安全是一门综合性学科，从传统的计算机安全到信息安全，不仅名称变更是安全发展的延伸，安全不是纯粹的技术问题，而是将管理，技术和法律问题相结合。

该专业培养高级信息安全专业人员，可从事计算机，通信，电子商务，电子政务和

电子金融。

信息安全主要涉及三个方面：信息传输的安全性，信息存储的安全性以及网络传输的信息内容的审计。身份验证身份验证是验证网络中主题的过程。通常有三种方法来验证主体的身份。一个是主体知道的秘密，例如密码和密钥;第二个是主体携带的物品，如智能卡和代币卡;第三是只有主题的独特功能或能力，如指纹，声音，视网膜或签名。等