浅析信息安全深度防御发展趋势

Brief Analysis to the Development Trend of Information Security Defense

■ 翟蒙 / 中国航发研究院

在全球网络规模不断扩大、信息技术获得巨大发展的今天，信息战争现实化、战场全球化、对抗常态化、网络攻击白热化的趋势越来越明显，维护信息安全已成为事关国家安全、社会稳定的大事。

随着信息技术的发展和普及，信息化给国家军事、社会和生活带来了极大的改变，信息数据已成为国家的重要战略资源。近年来，全球网络安全形势日益严峻，世界各国不断加强信息安全深度防御战略部署，网络格局已发生重大变革。在此大环境下，信息系统在数据采集、传输、存储、应用程序以及基础环境等各个层面，不断面临着非法访问、网络攻击、数据窃取等威胁，尤其央企、军工行业受影响更大，其中芯片、光刻机、航空发动机等又是国外重点关注对象，要维持信息系统安全、稳定运行，对信息安全防御能力有着很高的要求。本文通过对信息安全深度防御特点的分析，比较了美国、欧洲等发达国家和地区的信息安全政策、评估准则、体系建设等，并探讨了我国的信息安全政策、架构及后续规划。

全球信息安全防御现状

在全球一体化的背景下，信息化建设得到各国重视，许多国家、地区及组织越来越依赖信息系统，其中风险、收益与信息安全密切相关，成为信息管理的重要组成部分。近年来，网络攻击技术和攻击工具有了新的发展趋势，面对信息安全形势的日益严峻，世界各国高度重视信息安全保障，其中美国、欧洲的信息安全深度防御体系起步较早，完成度最高，对其他国家具有指导作用。

信息安全评估准则和标准建设

国际信息安全标准建设始于20世纪70年代中期，80年代迅速发展，90年代受到世界各国的关注。在80年代中期，为了满足军事电脑保密的需要，美国国防部（DoD）在20世纪70年代建设的基础上制定了新的可信计算机系统安全评估标准（TCSEC）。自美国国防部发布TCSEC起，各国也相继发布了自己的标准，如英国、法国、德国、荷兰在20世纪90年代早期公布的信息技术安全评估标准(ITSEC)、加拿大可信计算机产品评估标准（CTCPEC）、由英国标准协会（BSI）制定的信息安全管理标准BS779(ISO17799)和国际标准化组织（ISO）认可的SSE-CMM(ISO/IEC21827：2002)等信息安全管理标准。

到目前为止，美国已经开发了100多个满足TCSEC要求的安全系统，包括安全操作系统、安全数据库、网络组件等，然而这些系统仍有局限性，并没有真正达到安全系统的最高级别。因美国国防部制定的TCSEC准则仅考虑到保密性，所以英国、法国、德国和荷兰在ITSEC中加入了包含保密性、完整性和可

安全评估准则

颁布时间	国别	名称
1985年12月	美国	可信计算机系统安全评估标准（TCSEC）
1990年5月	法国、德国、荷兰、英国	欧洲信息技术安全评估标准（ITSEC）
1990年5月	加拿大	加拿大可信计算机产品评估标准（CTCPEC）
1991年2月	美国	美国联邦信息技术安全准则（FC）
1996年1月	北美及联盟	信息技术安全评价通用准则（CC）
1999年7月	ISO	批准CC为国际标准

用性概念的信息技术安全评估标准，但该标准并没有为上述问题提供一个全面的理论模型和解决方案。在TCSEC、ITSEC、CTCPEC、美国联邦准则（FC）等安全准则的基础上，由美国国家安全局和国家技术标准研究所、加拿大、英国、法国、德国、荷兰共同制定了信息技术安全评价通用准则（CC）。CC整合了现有国际评价及准则，并被ISO确立为国际标准。

信息安全保护法建设

网络和信息系统安全相关法律法规的建设也是美国关注的重点。2002年美国颁布了《联邦信息安全管理法案》（FISMA），FISMA定义了一个广泛框架，用于保护联邦政府的信息安全不被操控、破坏。欧盟对于信息安全保护法的颁布实施同样重视，早在1995年欧盟就颁布了《数据保护法》《电子签名法》《电子商务法》《网络与信息安全建议》《电子欧洲计划》等一系列法律法规，并在之后组建欧洲网络与信息安全局（ENISA），以指导和协调各个成员国的信息安全工作。欧盟委员会(European Commission)在2011年加强网络安全立法，以应对日益增长的网络攻击威胁。根据新规定，网络攻击者和相关恶意软件的制造者将被起诉，刑事处罚的上限将延长到两年。在发生网络攻击时，欧洲各国有义务迅速回应求助请求。法规还对非法拦截监听信息这一新的刑事犯罪进行了界定。

我国信息安全防御现状

防御措施

我国已将信息产业在国家中长期科学和技术发展规划纲要(2006—2020年)中列为11个重点领域之一，信息技术在今后能够起到支撑发展、引领未来的作用。加强网络与信息安全保障作为中国信息化建设的重要指导思想，是政府、部委、央企、金融及运营商等依据国家标准及各自的行业标准，基本逐步完成自己的信息安全技术体系建设和信息安全管理体系建设，达到国家和主管单位对于信息系统安全保障的基础要求。“十三五”期间，根据国家的政策、各行业的发展、面临威胁的变化，要求将信息安全发展向新的层级全面推进。

2016年11月，全国人大常委会通过了《中华人民共和国网络安全法》，其中规定“国家制定并不断完善网络安全战略、国家坚持网络安全与信息化发展并重、国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序”，说明我国对网络安全风险和威胁非常重视，对关键信息基础设施的安全非常关注。

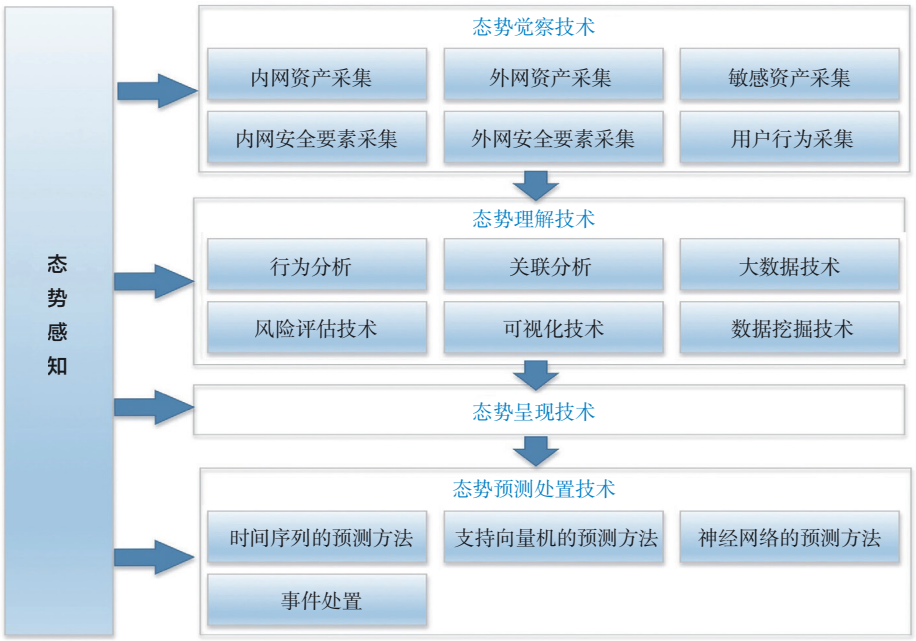
军工企业信息安全防御体系

军工企业是国防科技工业的重要组成部分，是国防综合实力的重要发展企业。作为世界第二大经济体，中国拥有完整的工业体系，但在芯片、航空发动机等诸多核心领域则是遭受国外打压、技术封锁最严重的领域。随着信息技术的全面发展，信息化建设已成为军工企业科研开发不可缺少的组成部分。近年来，我国国防实力不断提高，国防企业的综合实力不断增强，国内外敌对势力频繁通过信息窃取、网络攻击等方式想要掌握我国军工企业的生产、研究、开发、规划和发展信息。

为建立信息安全防御体系，我国采用信息系统安全等级保护、分级保护来验证信息系统是否满足相应安全保护等级，这是我国信息安全管理的一种有效方法。信息安全等级保护是信息技术发展和维护国家信息安全的根本保障，是国家在发展信息安全保护工作中下的决心。信息安全等级保护分为5个等级，其中，第一级为信息系统起到自主保护，第二级为信息系统能够指导保护，第三级为监督保护（对应分级保护第一级），第四级为对信息系统

信息安全相关法律法规

颁布时间	法律法规
2019年5月	网络安全等级保护制度2.0系列标准发布，包括《信息安全技术网络安全等级保护基本要求》《信息安全技术网络安全等级保护测评要求》《信息安全技术网络安全等级保护安全设计技术要求》
2019年5月	国家互联网信息办公室发布《网络安全审查办法(征求意见稿)》
2019年6月	工业和信息化部发布《网络安全漏洞管理规定(征求意见稿)》
2019年7月	《云计算服务安全评估办法》
2019年9月	《工业大数据发展指导意见(征求意见稿)》
2019年10月	《中华人民共和国密码法》



态势感知的安全处理流程

及应用系统的强制保护（对应分级保护第二级），第五级为对系统的专控保护（对应分级保护第三级）。分级保护是根据信息的重要性和信息的最高安全等级来确定保护等级。通过等级保护和分级保护，提出了各级信息系统的技术要求和管理要求。技术要求包括身份认证、访问控制、数据完整性、审计等。管理要求主要是考核相关制度、人员管理，逐级提高防护要求。

军工企业信息安全防护按照国家保密局分级保护标准建设，《“十三五”国家信息化规划》中失泄密监管系统要求，重点加强监测预警体系，有效防止内部用户有意或无意的泄密行为，有效应对来自国内外敌特组织的高级持续攻击，实现网络防护监管一体化，支持网络的主管部门和运行维护部门对涉密网络进行自监管。包括从人员、管理、技术等3方面持续改进管理和技术体系，保证网络物理隔离、终端管控、网络分区与边界防护、应用系统防护、权限控制和知悉范围管控、三员权限分离等基础防护的持续有效；在涉密网络互联、涉密网日常运行过程中，及时发现和处置失泄密行为、网络安全攻击事件、不合规操作和配置等，通过定期的安全审计、风险自评估、监督检查等手段识别和处置网络安全风险。

深度防御技术特点及发展趋势

现代信息安全在保证信息真实、完整、有效的同时，还要将信息系统建设成为集保护、感知、理解、预测和响应为一体的深层次防御体系。信息安全深度防御技术从传统的被动防御逐渐向监测响应型防御发展，并从整体上向系统化、主动防御方向发展，安全产品间的自适应联动保护增强，是一个基于态势感知的安全处置流程。该防御系统实时关注的主体有：计算机进程、存储的各种文件、通信时交换的信息、所有操作记录和用户指令等，该系统还要有一个独立的系统防卸载模块，以提高系统的可靠性。

态势感知广泛应用于军事、航空航天、网络安全等领域。基于态势感知的安全处理流程包括首先收集关键信息，然后利用这些信息对系统进行分析和理解，最后由决策者进行预测处理。基于态势感知的安全解决方案对应分析中心、监控中心和运维中心3部分。分析中心完成态势感知数据的获取和分析，监控中心完成态势感知的理解，包括对当前网络状态和历史网络状态的分析，运维中心完成态势感知和安全事件处理。实时采集企业内部网络和外部网络感知数据，使决策者能够及时检测威胁，掌握整个系统的安全状态，统一应对威胁，准确判断安全级别，并做出相应的应急响应。处理结果将直接反馈给分析中心和监控中心，以了解安全问题是否得到了妥善解决，从而更有效地提高安全水平。

结束语

信息安全问题已成为社会关注的焦点，信息安全深度防御系统已成为整个社会经济和企业生存发展的重要基础。国外信息安全之路已经发展了几十年，从早期零散、随意的标准，发展为系统化、层次化、覆盖全生命周期的信息安全管理体系。借鉴国外先进经验和理论，结合我国实际，在实际工作中灵活运用，能有效提高我国特别是航空发动机领域的信息安全深度防御水平。 航空动力

（翟蒙，中国航发研究院，工程师，主要从事网络安全技术研究）