

浪潮产品安全白皮书

浪潮端到端的产品安全保障体系和实践

浪潮电子信息产业股份有限公司

2021年2月

inspur 浪潮



目录

1 序言	01
2 执行摘要	02
3 浪潮端到端的产品安全实践	03
3.1 端到端的产品安全保障体系	03
3.2 产品安全组织架构	05
3.3 开发安全	07
3.3.1 概述	07
3.3.2 安全需求分析	07
3.3.3 安全设计	08
3.3.4 安全开发	08
3.3.5 安全测试	08
3.3.6 安全发布	09
3.3.7 配置管理	10
3.4 第三方组件安全治理	11
3.5 独立安全测评	12



3.6 供应链安全	13
3.6.1 概述	14
3.6.2 供应商及物料安全	15
3.6.3 生产制造安全	16
3.6.4 仓储物流安全	17
3.7 交付安全	18
3.8 安全事件响应	19
3.9 组织安全能力保障	20
3.9.1 信息安全	21
3.9.2 个人隐私保护	22
3.9.3 安全赋能培训	23
3.9.4 内部审计/审核	24

4 未来展望	25
---------------	-----------

5 关于浪潮信息	26
-----------------	-----------



1 序言

当今，我们正处于数字化、智能化、网络化的新时代。信息和通信技术（ICT）的发展和普及，对全球经济、人类社会发展发挥着基础性和引领性的作用。但是，我们也看到，当前全球范围内的网络安全威胁日益复杂多变，这些威胁不受时空限制，给网络安全带来了极大的挑战。

数据中心是数字经济发展的关键信息基础设施，支撑着数据存储、处理和流通，其安全性至关重要。因此，各国政府、服务提供商和运营商、企业、用户都非常重视网络安全。浪潮作为全球智慧计算的领先者，为云计算、大数据、人工智能提供先进算力平台支撑。我们深知所提供的产品和服务的安全性对保护客户资产和用户数据安全的重要性。因此，我们制定了产品安全策略，并将安全作为公司产品开发和交付最高优先级任务之一。

浪潮电子信息产业股份有限公司（以下简称“浪潮”或“公司”）产品安全的目标以客户为关注的焦点，致力于为客户交付安全可靠的产品和服务。浪潮根据公司发展战略规划，遵守适用的法律法规，参考国际、相关国家和地区的网络安全标准和业界最佳安全实践，建立并实施先进的端到端产品安全保障体系，不断提升全员网络安全意识和能力，以我们最大的努力确保为客户持续提供安全可靠的产品和服务。

同时，我们也深刻理解产品网络安全治理是一项复杂的工作，需要通过产业链上下游和其他利益相关方的共同合作，才能应对日益严峻的网络安全挑战。浪潮愿以开放、透明的方式，与各方开展沟通和协作，持续改进管理和技术实践，不断完善产品安全保障体系。我们也欢迎大家反馈宝贵的意见，帮助我们能更好的改进流程和技术，以便为客户提供更好的产品和服务。



2 执行摘要

当前，我们正处于一个万物智能互联的数字化时代，数据洪流汹涌而至，孕育着前所未有的巨大机遇。数据中心是数字经济发展的关键信息基础设施，帮助各行各业应对数据洪流，最大程度的挖掘数据的价值。在过去十几年来，不断涌现的新型计算技术推动着数据中心计算力的持续提升，并深度融合到国家治理、经济和社会发展的方方面面。新技术的创新和应用极大地促进了经济社会发展的同时，网络安全形势也越来越严峻。

据世界经济论坛发布的《2019年全球风险报告》¹数据显示，从风险发生的可能性来看，数据欺诈或盗窃、网络攻击分别位列前十大风险的第四位和第五位；此外，报告还提到，关键信息基础设施存在的严重安全漏洞已发展成为国家安全问题，以及人工智能和物联网等新技术带来了更多不确定性的安全风险，这些都增加了网络攻击的风险。另外，根据美国国家漏洞库（NVD）²基于CVSS V3对已公开披露的6.7万余个漏洞的评分来看，致命漏洞占比约15.4%，高危漏洞占比约43.7%，两项合计占近60%。

网络安全工作没有“银弹”，也没有“终点”，没有什么技术和方法可以实现100%的安全；但是我们可以做到的是通过产业链上下游和其他利益相关方的合作和共同努力，积极完善产品安全保障体系，尽可能消减产品安全漏洞，提升安全事件响应速度，以减少网络安全事件给我们带来的不利影响。

正如期望的那样，我们也积极加强同客户和利益相关方的沟通，并通过实践来不断完善我们的产品安全保障体系，以我们最大的努力确保为客户持续提供安全可靠的产品和服务。

一年以前，在第一版产品安全白皮书——《浪潮服务器产品安全白皮书》中，我们从服务器产品安全的角度详细阐述了我们产品安全保障体系的基本策略、框架、技术和方法，以便让客户和公众了解我们在网络安全方面所做的努力。通过一年多来的沟通和实践，我们的产品安全实践得到了客户的普遍认可。但随着我们产品安全实践的不断深入和内外部环境快速变化，我们也发现了很多需要改进的方面。

本白皮书中，我们将以客户的关注为出发点，更加全面地、系统地阐述浪潮端到端的产品安全保障体系。这也充分体现了我们在产品安全工作方面的持续改进的能力。

1. http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

2. <https://nvd.nist.gov/general/nvd-dashboards>

3 浪潮端到端的产品安全实践

3.1 端到端的产品安全保障体系

浪潮建立并实施了端到端的产品安全保障体系来推进产品安全建设工作，以尽我们最大的努力为客户交付安全可信赖的产品和服务。端到端的产品安全保障体系的输入端是各类客户和其他利益相关方的安全需求，输出端是通过交付安全可信赖的产品、方案和服务来满足其安全需求。产品安全保障体系覆盖安全策略与流程、工程过程安全、安全技术、组织与人员安全等多领域多维度，从而构建产品全生命周期安全保障体系，如图3-1所示。

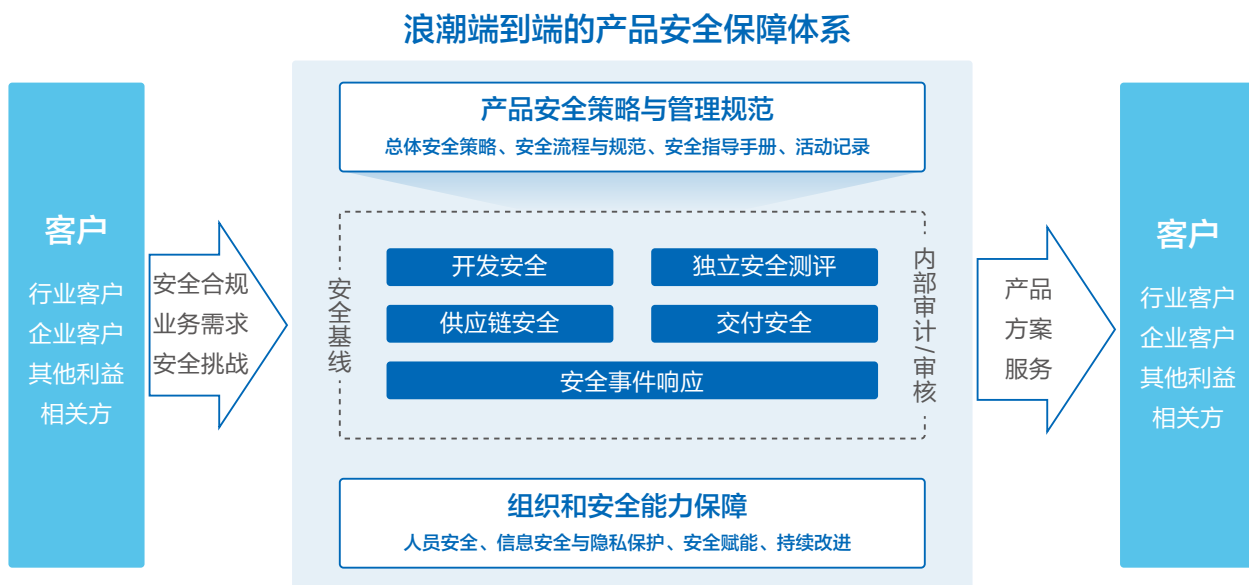


图3-1 浪潮端到端的产品安全保障体系

产品安全策略与管理规范

安全性已成为我们产品基本属性之一。为满足这一要求，我们制定了产品总体安全策略，对产品安全建设提出了基本要求，即“安全基线”。同时，我们还制定和发布了配套的安全管理规范、流程、标准和指导手册，各产品业务单元按照统一的标准开展产品安全工程活动，并输出相应的结果和记录，作为相关方审计的证据。

开发安全

浪潮IPD产品开发流程是产品研发领域共同遵循的流程，在追求高效研发的同时，我们也更加注意产品的安全。我们已将安全内建于产品规划、需求分析、设计开发与验证、发布与维护等产品全生命周期过程中，以确保产品工程过程的安全。



独立安全测评

除了在产品开发阶段进行安全测试外，我们还建立了独立的安全测评团队，以第三方的视角对产品进行独立安全性测评，从而为产品安全验证构建第二道安全屏障；同时，我们也积极与独立第三方产品测评/认证机构和人员合作，对我们的产品进行客观公正的安全评估。

供应链安全

浪潮是全球领先的IT基础架构技术、产品、方案和服务供应商，其供应商遍布全球。产品供应链安全是一项复杂的工程，需要产业链上合作伙伴的通力协作，共同应对面临的网络安全风险。浪潮参考国际标准和业界最佳实践，结合自身现状，在供应商与物料引入、生产制造、仓储和物流等领域采取了一系列网络安全控制措施，确保产品的完整性、可用性和真实性，降低产品被篡改和假冒的风险。

交付安全

产品设计和开发安全做得再好，如果在客户现场的部署或维护方式不安全，那最终安全效果也将大大折扣。因此，确保交付安全也是产品全生命周期安全保障体系重要部分之一。浪潮从技术和管理两个维度不断提高水平，从而确保我们交付的产品和服务尽可能安全。技术上措施包括对固件或软件进行完整性和真实性验证，补丁升级、故障定位等等；管理上措施包括从交付流程和规范，安全配置指导，人员安全技能和行为规范等。

安全事件响应

受多方面客观因素的影响，产品自身的脆弱性不可能完全消除，外部威胁也在不断发展变化，当潜在安全风险转变为安全事件时，就需要及时有效地进行安全响应，并与客户和其他利益相关方开展合作，确保快速安全地把系统恢复到期望的状态，以减少安全事件的不利影响。浪潮秉承公开透明的原则，遵循国际安全事件/漏洞处理相关标准，建立了完整的安全事件响应机制，确保产品漏洞信息得到及时披露，以及提供有效的产品漏洞修复解决方案。

组织和安全能力保障

组织环境、IT系统和人员是驱动产品安全的重要因素，特别是人员安全意识和能力不足将直接影响产品安全的效能。浪潮基于ISO/IEC 27001、ISO/IEC 27701等建立了完善的信息安全和隐私保护体系，并通过相关认证。我们还建立了完善的人员安全培训和认证体系，确保关键岗位安全意识和能力的持续提升。此外，我们还与独立第三方机构合作，基于相关安全标准和业界最佳实践对产品安全保障体系和相关活动的执行进行评估，并推动持续改进工作。

3.2 产品安全组织架构

为确保产品安全保障体系融入产品规划与管理、设计与研发、供应链、生产制造、产品交付、技术服务等产品全生命周期，保证产品安全策略得到有效地实施，我们建立了自上而下的多级产品安全组织架构，并为每个安全团队赋予清晰的责任。浪潮产品安全组织架构如图3-2所示。

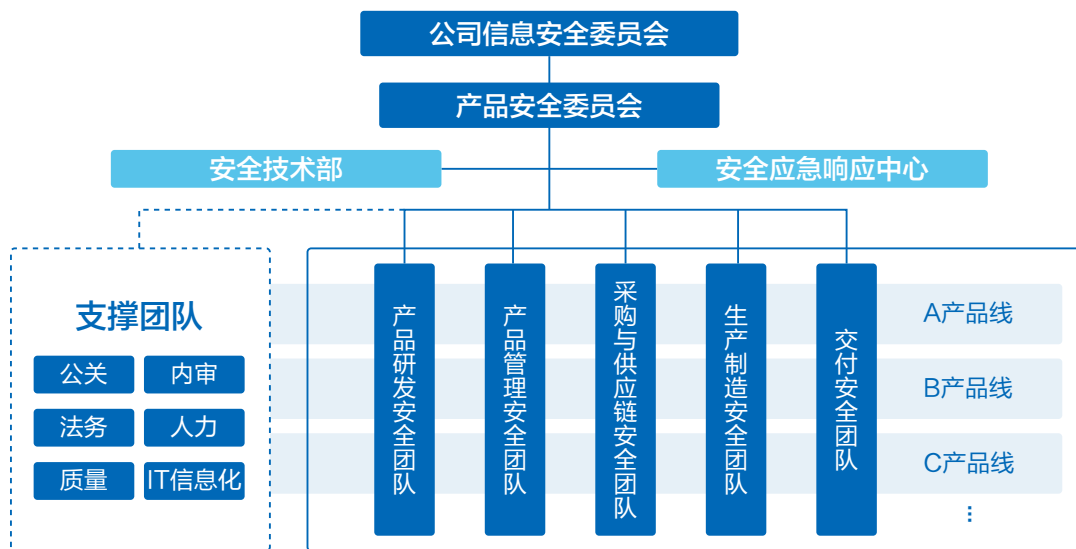


图3-2 浪潮产品安全组织架构

公司信息安全委员会

作为公司信息安全的最高决策和管理机构，负责制定公司网络信息安全总体策略，统一规划信息安全管理体制、规范和执行标准，协调、督促各部门的信息安全工作。


产品安全委员会

是公司信息安全委员会领导下的，专门从事公司产品网络安全建设的委员会，由公司高层和业务线负责人组成的管理团队，负责公司产品网络安全总体规划、政策的制定，冲突和重大问题的决策。

安全技术部

是产品安全委员会的常设机构，负责落实公司产品网络安全总体策略，制定产品安全基线，以及配套的产品安全管理规范、流程、标准和指导手册，并作为内部独立组织监督和审核各产品线安全活动的执行。

负责独立的内部第三方产品安全测评，识别与分析产品可能存在的安全漏洞和风险，协同开发团队制定合理可行的安全修复方案，确保产品符合安全发布准则。



专注于服务器、存储和云计算等领域的安全标准、安全攻防技术研究，产品公共安全模块（CBB）的研究与开发。

负责组织网络安全意识、安全技术能力的培训与认证。

安全应急响应中心

作为浪潮产品安全应急响应团队，负责接收、处理和公开披露产品安全漏洞，并与产业链上下游、公共组织等开展交流与合作，持续为客户提供安全服务。

产品研发安全团队

遵照共同的产品安全研发流程和规范，开展相关安全要求在产品线中的需求分析、设计与研发、测试和发布等过程的落地实施，对产品研发全过程的安全负责。

产品管理安全团队

负责识别、分析产品业务线规划目标客户所在国家和地区、行业的网络安全合规要求和业务场景安全需求，开展产品线短期和中长期规划。

采购与供应链安全团队

负责建立物料、供应商和仓储物流网络安全管理体系，持续开展物料、供应商和仓储物流的网络安全风险评估，并监控、完善和优化安全控制机制。

生产与制造安全团队

负责建立严格的安全生产管理体系、操作规范和应急预案，强化安全生产和产品设计的一致性，切实做到安全生产，确保为客户提供高质量、安全可靠的产品。

交付安全团队

负责建立产品安全交付流程规范，产品安全指导手册，交付人员安全技能培训，并为客户提供优质、安全的产品交付和售后支持服务。

支撑团队

负责提供与产品安全相关的公关、法务、质量、内审、人力及IT信息化等方面支持工作。

3.3 开发安全

3.3.1 概述

浪潮IPD产品开发流程是产品研发领域共同遵循的流程，在追求高效研发的同时，我们更加注重产品的安全。安全性已成为产品的基本属性之一，已内建于产品开发生命周期全过程中，确保始终能为客户持续交付安全、可信赖的产品和服务的能力。

浪潮基于多年来的开发安全实践，并参考业界最佳安全模型和国际安全标准，如BSIMM、微软SDL、ISO/IEC 27034等，在IPD产品开发流程中同步定义了安全需求分析、安全设计、安全开发、安全测试、安全交付与维护等安全活动，确保各类安全指标有效地内建到产品开发活动中，如图3-3所示。同时，公司组建了独立的安全组织，积极开展先进安全技术研究，持续进行安全活动度量和改进，并通过完善的研发安全培训与认证体系开展安全赋能，为安全活动的有效执行提供保障。

安全活动内建于浪潮IPD流程

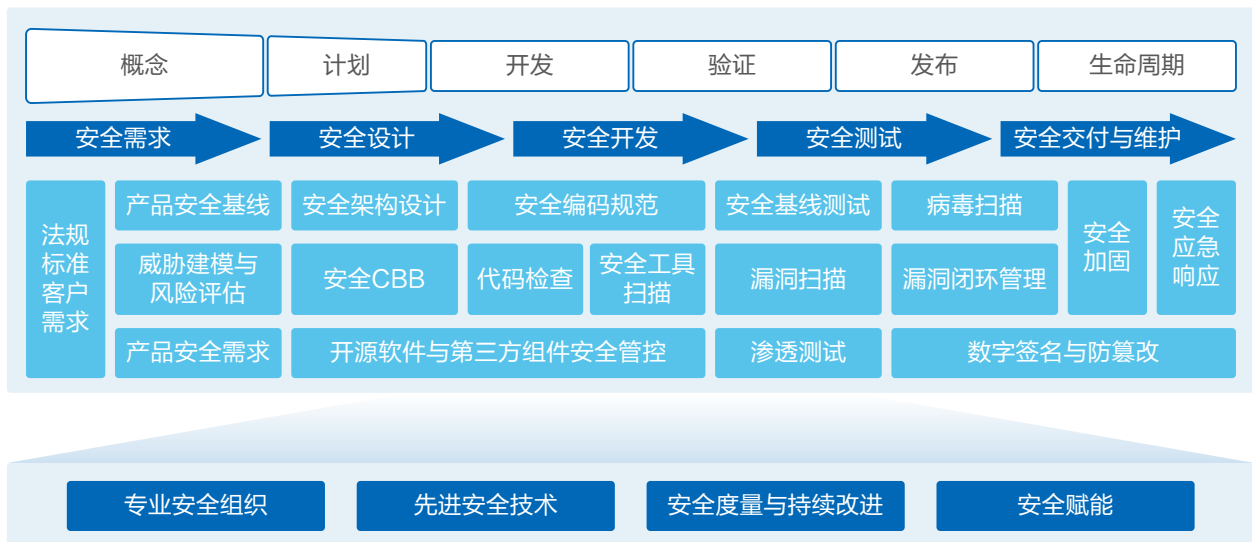



图3-3 浪潮安全开发流程

3.3.2 安全需求分析

在产品概念阶段，浪潮结合市场准入需求（如相关的法律法规、各领域安全标准）、客户应用场景安全需求、行业需求、同行经验、公司内部安全基线等，将中长期安全需求纳入产品路标规划，短期安全需求纳入产品版本规划。



在产品版本规划中，产品安全需求主要包括两部分，一是公司产品安全基线需求，作为需求强制执行；二是基于产品应用场景进行风险评估形成的补充安全需求。无论是安全基线需求还是补充安全需求都将纳入产品需求池进行统一管理和跟踪，确保安全需求得到有效的落地。

1) 产品安全基线需求：我们遵循各领域相关安全标准及最佳实践，针对不同类型产品制定相关基线需求，并进行定期的维护和更新。产品安全基线需求作为必选的需求纳入产品需求中强制执行。

2) 补充安全需求：主要结合产品应用场景（区域、行业、特定安全保护要求等因素），采用风险评估的方法，识别产品面临的威胁，确定产品应采取的安全防护措施。

3.3.3 安全设计

浪潮参考ISO/IEC 15408、GB/T 18336、STRIDE等安全标准和业界最佳实践，制定了产品安全设计规范，各产品研发团队依据产品安全设计规范进行产品的安全架构设计、特性安全设计。

根据产品应用场景，设计人员分析系统的安全需求和潜在的安全风险，确定产品的安全架构和系统方案，确保满足市场和客户安全要求。设计人员还需要通过威胁建模的方法来分析设计方案的安全性，以便在早期阶段发现潜在的安全威胁并加以控制。

在第三方组件选型时，需要由专业安全团队对第三方组件进行安全风险评估，确保符合公司第三方组件准入要求。此外，针对产品所需的通用安全模块（如身份鉴别、输入安全检查等），统一由专业安全团队来开发和维护，确保了安全模块的自身安全性。

3.3.4 安全开发

在开发阶段，浪潮参考业界权威的代码安全规范和最佳实践，如OWASP（开放式Web应用程序安全项目）、CERT（计算机安全应急响应小组），制定了覆盖C/C++、Java、Python等多种语言的安全编码规范。开发人员在代码实现过程中需遵守统一的安全编码规范，并针对重要代码进行人工检查。

同时，我们还制定了《代码安全扫描管理规范》，要求开发团队在此阶段使用商用和自研源代码扫描工具对代码进行白盒和黑盒安全检查，并将发现的安全缺陷纳入缺陷管理系统进行统一管理和跟踪，确保代码安全缺陷得到有效的修复。

此阶段，我们还需要通过商用开源软件合规检测工具对软件中使用的开源软件进行合规性评估，确保符合开源软件相关协议的要求。

3.3.5 安全测试

为确保产品符合安全需求规格定义的要求，在测试阶段，我们要求制定安全性测试方案，设计并执行安全测试用例，对产品所有安全功能进行测试和验证，防止因设计或编码不当导致的安全效能不达标的问题。

除了对安全功能进行测试外，我们还需要对产品进行病毒扫描、漏洞扫描、通信矩阵符合性测试、协议健壮性测试、渗透性测试等工作，针对存在的安全问题进行整改，确保安全风险得到有效的缓解。

3.3.6 安全发布

在产品发布阶段，我们制定了严格的安全出口指标（如安全需求达成指标、安全缺陷修复指标、安全活动执行指标等等），只有达到安全出口指标方可进入发布流程。

此外，我们还采用多种主流杀毒软件对产品进行检查，确保发布版本无异常。同时，我们还对关键软件/固件进行数字签名，保证从产品发布、生产制造、产品交付整个过程的真实性和完整性。

3.3.7 配置管理

浪潮产品研发配置管理参考了CMMI、ISO/IEC 15408等标准，建立了完善的配置管理流程，并采用了自动化平台，对产品开发生命周期进行标识组织和控制。配置管理严格按三库（开发库、受控库、产品库）的要求管理，并制定了严格的数据备份机制。

浪潮配置管理目标是保证产品和研发过程的完整性、一致性、可追溯性。

完整性

- 1) 产品配置库纳入所有自研/开源代码、文档、基线、执行程序、安装包、版本说明等；
- 2) 统一管理和使用第三方软件库和工具。

一致性

- 1) 版本由构建中心自动编译、构建，无人工干预，确保源代码与目标程序一致性；
- 2) 发布软件包/固件全部生成摘要值或数字签名，可有效支持客户环境时部署版本的完整性与真实性检验。

可追溯性

- 1) 所有变更保留完整和准确的记录，如变更原因，变更人员，审批人员，对应的需求等信息；
- 2) 具备产品组件追溯能力，当发现产品安全缺陷时，可迅速定位关联产品或版本。

3.4 第三方组件安全治理

浪潮对需要使用的第三方组件（包括开源软件、第三方商用软件/组件/部件等等）制定并实施了全生命周期的安全管理措施，从这些组件的引入，集成开发，直到作为产品的一部分向客户交付整体过程。我们将第三方组件的合规性评估、安全风险评估、安全测试、漏洞管理等活动内建于浪潮IPD流程中，确保第三方组件的使用和维护都能得到有效的安全管理。

我们将第三方组件作为配置项，纳入配置管理流程，确保可以追溯第三方组件的使用，一旦发现安全漏洞，会对漏洞进行评估，并提供解决方案或者规避措施。此外，浪潮积极加入开源社区（如Openstack）并持续跟踪开源社区发布的漏洞，提交安全漏洞修复方案，积极为开源组件的安全作出贡献。

3.5 独立安全测评

为尽可能降低产品发布前的安全缺陷，除了在产品开发阶段进行安全测试外，我们还建立了独立的安全测评团队，以第三方的视角对产品进行独立安全性测试，从而为产品安全验证构建第二道安全屏障，最大程度上降低产品存在安全缺陷的可能性。此外，安全测评团队对产品发布具有一票否决权，从机制上确保产品安全缺陷进得有效的控制。

安全测试团队在独立的安全性测评过程中，主要从安全开发过程评估、产品安全性测试等方面开展工作。

安全开发过程评估

对开发过程中执行的安全需求分析、安全设计、源代码安全检测、安全功能测试、安全性测试等安全活动进行分析和评估，确保产品安全需求在相关文档中说明是完整的、一致的，符合公司对每个阶段安全活动定义要求。

安全性测试

- 1) 人工代码安全检查：参考业界主流软件TOP风险/脆弱性（如OWASP TOP10、CWE TOP25等），通用人工方式对关键源代码进行正向和逆向安全分析，弥补自动化安全工具不易识别的代码安全问题。
- 2) 安全扫描：采用业界主流商用安全扫描工具，对产品安全性测试进行再验证，如自研代码和第三方组件安全漏洞，安全配置漏洞，未声明的外部接口和账号等等。
- 3) 渗透测试：基于模拟攻击方式，对产品进行渗透性测试。分析产品应用场景及可能存在的脆弱性，采用自动化工具渗透、人工渗透、模糊测试等多种方式，挖掘产品存在的安全漏洞，对发现的安全缺陷进行分析，并提供改进建议。

此外，我们还积极与各国和各地区独立第三方产品测评/认证机构和人员合作，对我们的产品进行客户公正的安全评估。

3.6 供应链安全

3.6.1 概述

浪潮非常重视产品供应链安全，并将其作为降低产品被假冒、嵌入恶意软件或被篡改风险的重要抓手。浪潮参考ISO/IEC 28000、ISO/IEC 27036、ISO/IEC 20243(O-TTPS)、ISO/IEC 9000等相关标准，识别和评估产品全生命周期的安全隐患，通过安全管理流程降低产品真实性和完整性被破坏的风险，将产品安全的要求嵌入到供应商及物料管理流程、生产制造流程、仓储物流流程中，建立了产品安全追溯和识别能力，并确保有效运行与持续改进。浪潮供应链管理流程如图3-4所示。

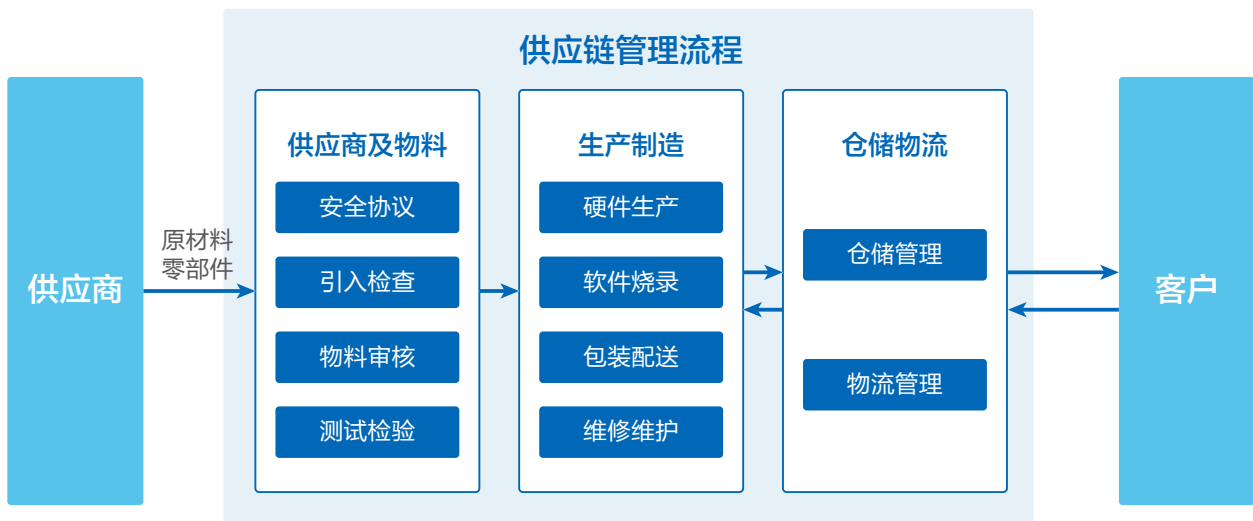


图3-4 供应链管理流程

浪潮供应链安全管理围绕三个核心特性开展相关工作：

- 1) 完整性——在整个供应链中，最大程度地减少产品和服务被恶意篡改、假冒带来的风险，尽早识别并解决威胁，保障产品和服务的完整性。
- 2) 可追溯性——实现全流程追溯，建立高效的可追溯机制，包括软件、固件组件、硬件追溯，迅速定位产品或流程相关的漏洞或缺陷，确保及时响应和改进。
- 3) 有效性——确保供应链安全管理流程遵从法律要求和业界标准，推动供应链安全管理流程切实有效开展，促进安全需求有效传递和落实到供应链的各个层次。

3.6.2 供应商及物料安全

根据业务流程、质量管理及信息安全的要求，我们制定并完善针对供应商的风险评估方法，对供应基础进行广泛的审查，从零部件层面到物流合作伙伴。

公司建立了供应商引入安全评估管理制度。在与供应商合作之前，由专业团队从技术、商务和品质三方面对供应商开展引入核查。我们制定了供应商评估调查表，从信息安全、隐私保护、产品安全开发与交付等方面对供应商进行评估和核查。浪潮供应商引入核查模型如图3-5所示。

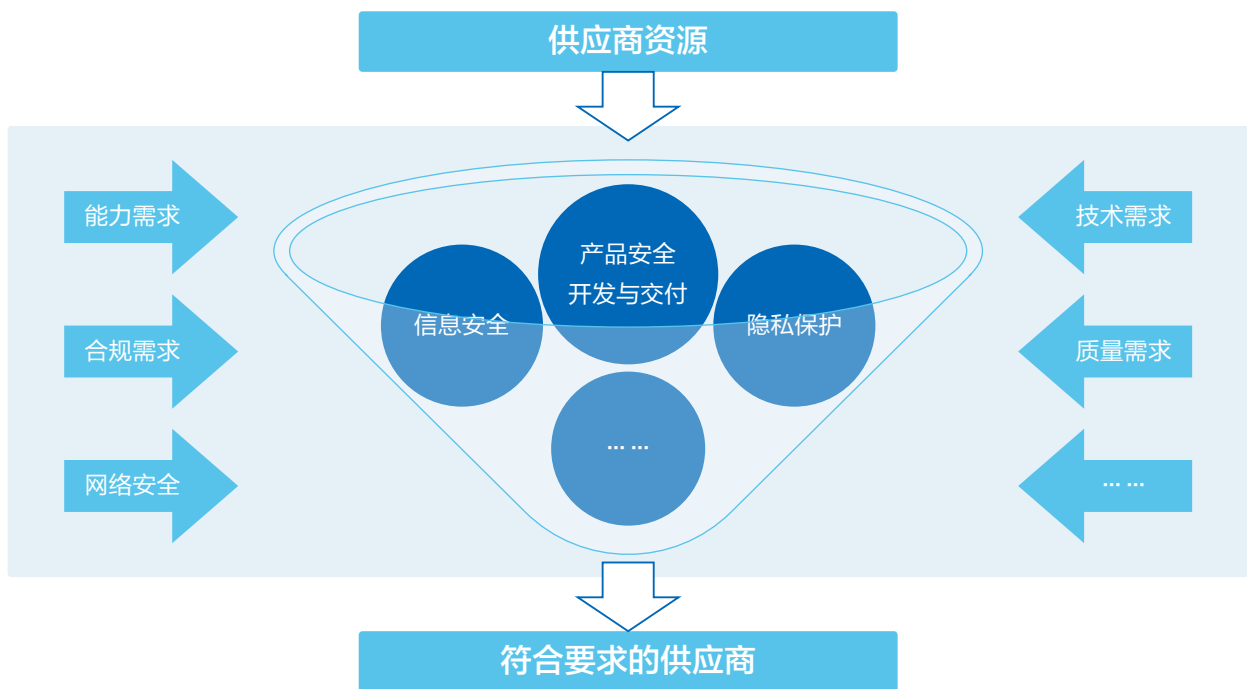


图3-5 供应商引入检查模型

在成为浪潮的正式供应商之前，供应商需签订相关安全协议或合同。安全协议或合同中包含了体系安全要求、产品安全要求、服务安全要求和违约责任等多个领域，具体要求包括但不限于法律责任及义务、保密责任、安全管理遵从、审计权、安全漏洞披露、合规性证明等，保证将安全需求落实到供应链的各个层面。我们定期对供应商进行风险评估，并监督和指导供应商不断改进和提高安全水平。

公司高度重视供应商物料安全检测，制定了物料安全规格。所有物料在入库前都需经过正式的物料接收、编码、评估、分发等流程控制。重要物料均需进行安全测评，经过严格的安全审核和信息记录。在来料接收环节，对接收到的物料与认证时的物料，进行再验证，确保其完整性。物料安全是供应商准入的必要条件之一。

3.6.3 生产制造安全

浪潮结合ISO/IEC 9000和ISO/IEC 27001，形成规范、高效、高质量和安全的生产体系，按文件和规范作业已经融入到生产制造的各个环节中，形成了严谨规范、重视质量、安全高效、不断改进的制造文化，确保为客户快速提供高质量、安全可靠的产品。

目前，浪潮已经在中国、美国、匈牙利等全球多地部署了生产基地和全球一体化的服务体系，为客户提供供应链对接平台，从需求到中间生产、交付，整个环节都可以清晰的看到，客户可以及时掌握整个项目节奏和风险，双方可以第一时间采取安全措施避免或缓解风险带来的影响。

在产品的生产过程中，浪潮采用多种方式确保从来料到发货的全过程安全可靠。在保证信息的完整性方面做了许多努力：服务器中每个部件在每个生产环节都会有两次信息采集，包括基于芯片的自动采集和基于电子扫描枪的人工采集；在整个生产制造过程中，对于软件发布、跨环境传输等情况，均会进行完整性校验。

3.6.4 仓储物流安全

在仓储物流方面，浪潮采用智能仓储系统（WMS）、运输管理系统（TMS）等信息系统，连接生产设备、人和物料，对产品的仓储和物流进行管理，并配合物料管理机制，实现物流、仓储、生产等全流程的自动化和可感知，从物料采购到成品交付的端到端的弹性、透明和可追溯。

为了满足客户期望，浪潮为供应商、物流伙伴制定了仓储及物流相关的安全规范，对在保护产品完整性方面提出要求，包括子供应商管理、防篡改包装、装箱规定、物理安全、物流跟踪等。浪潮制定了安全区域内的工作规程，对区域的出入口采取访问控制。设置安全管理员，进行日常监管、实施区域内的安全管控措施。浪潮还对相关岗位上的人员进行审查和意识、技术、管理上的安全培训，以避免人为操作因素而产生的风险。

3.7 交付安全

产品设计和开发安全做得再好，如果在客户现场的部署或维护方式不安全，那最终安全效能也将大大折扣。因此，确保交付安全也是产品全生命周期安全保障体系重要部分之一。产品安全交付要解决的关键问题是如何将产品安全地适配到客户应用场景中，并持续保持健康的状态。浪潮根据法律法规要求，以客户需求为出发点，参考业界相关标准与实践（如ISO/IEC 27001、ISO/IEC 27036），从安全技术、安全流程规范和人员安全三个维度建立了安全保障措施，从而确保我们交付的产品和服务尽可能安全，如图3-6所示。

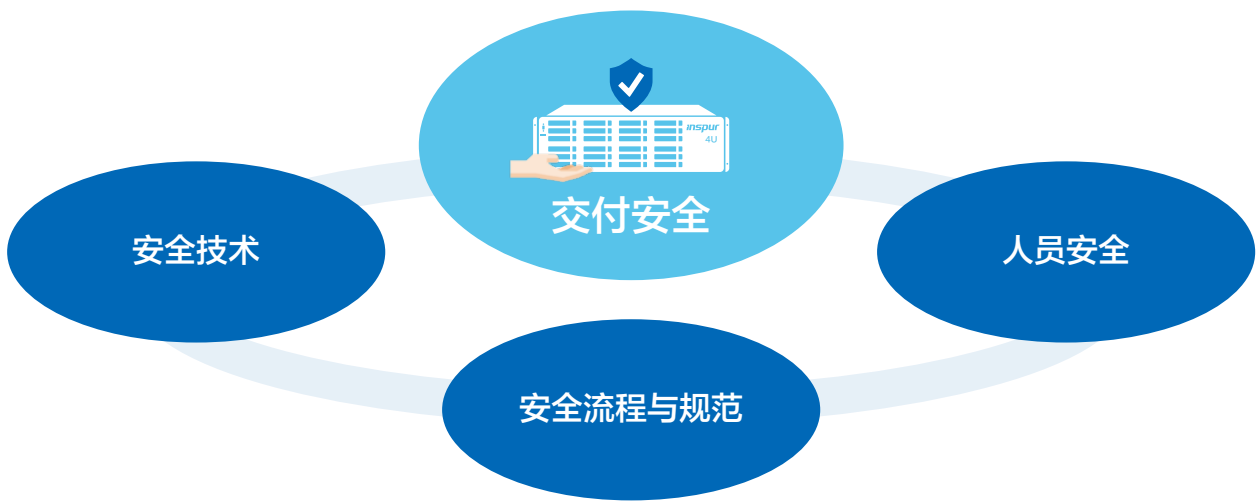


图3-6交付安全三个维度

安全技术措施

主要指内建于产品中，确保产品安全地部署和运行各类安全特性，包括部署前和运行时的完整性和真实性验证技术、补丁升级、故障定位、日志审计，并提供产品相关安全特性的详细配置手册。

安全流程与规范

从工程交付周期的角度，对每个阶段应执行的安全活动和遵循的安全策略进行了定义。这些流程与规范是可验证的、可重复的，为我们持续改进我们的交付质量提供了很好的基础。

人员安全

是交付安全的关键，因为任何交付活动都是由人来执行的。为确保交付人员和运维人员的安全，我们主要从三个方面开展了工作，一是人员持证上岗，确保交付人员具备专业能力；二是人员行为准则，确保交付过程的安全合规；三是人员赋能培训，确保交付和运维人员理解产品安全能力，掌握产品日志安全维护和应急处理相关技能。

一个完整的项目交付涉及交付准备、现场部署、验证与移交、维护支持等四个阶段。根据交付安全流程与规范，我们在交付每个阶段都设置了相应的安全活动和检查点，以及相关技术和操作指南支撑，以确保整个交付过程的安全，如图3-7所示。

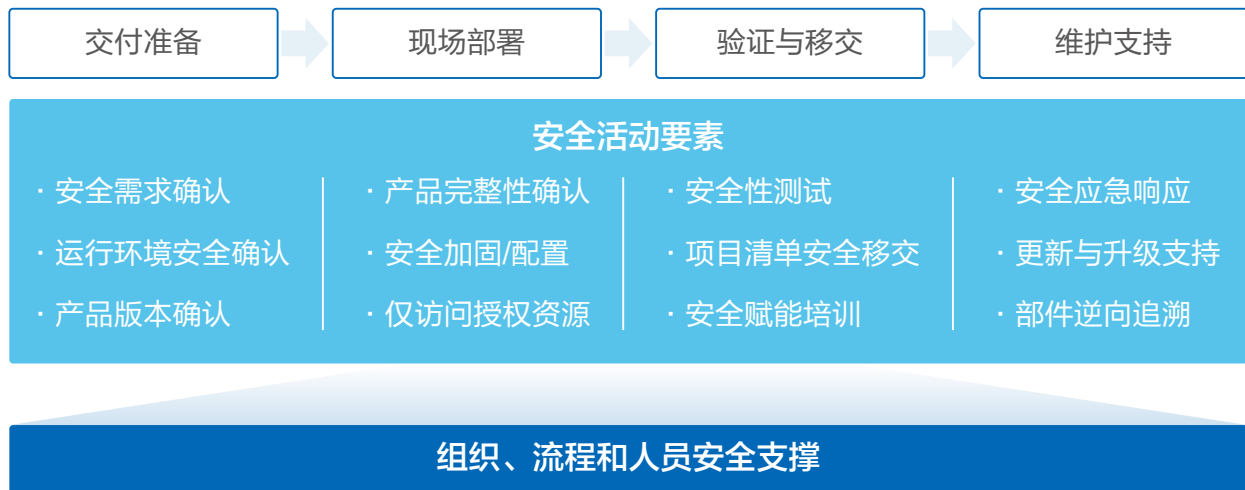


图3-7 交付安全活动要素

产品交付的四个阶段：

交付准备

该阶段是根据合同/协议要求，确认产品交付的安全需求，同时根据现场运行环境的不同，与相关方对部署方案进行优化，以确保产品最佳的安全运行参数。在此阶段，还需要对到货产品版本进行检查，可通过更新补丁或升级至最新版本，确保部署的产品不存在已知安全缺陷。

现场部署

软件产品或内含软件/固件的产品，从发布到生产制造阶段，我们均采用了完整性验证措施。同样，在将产品转移至客户现场时，我们采用了同样的完整性检查措施，以防止产品转移过程中潜在的篡改和污染安全风险。

产品发布时，我们尽可能遵循“默认安全”的原则，但客户应用场景和安全需求是千变万化的，因此，我们提供了详细的安全配置/加固手册，以帮助客户在业务和安全方面找到最佳平衡点。

此外，在部署的过程中，服务人员难免会接触到客户的网络和信息。我们要求服务人员对它们的任何访问和操作都需获得客户的明确授权，而且遵守相关的法律法规。

验收与移交

验收是确认产品符合要求的重要过程，安全性测试也是其中重要的内容，如漏洞检测、安全配置检测、开放服务检测等等。我们通过交付准备、现场部署两个阶段的安全活动执行，可最大程度上确保此阶段安全缺陷得到有效的控制。

产品移交不光涉及设备、软件、文档等有型资产的移交，还包括如何确保产品持续保持安全健康状态的技能移交。这就需要通过产品安全赋能培训，通过培训我们尽可能让客户相关人员理解产品安全能力，掌握日常维护技能和出现安全问题后如何获取支持。

维护支持

维护阶段才是产品和服务真正发挥价值的开始，也检验产品是否具备持续安全保障能力的“试金石”。我们都知道，产品所运行的环境随着业务和技术发展而变化，新的攻击形式和漏洞也在不断发展。因此，为了确保我们交付产品和服务的持续安全能力，我们建立了完善的安全事件响应和故障处理流程，包括持续监控互联网安全态势，与供应商和第三方安全机构保持密切合作，及时进行预警，并提供有效的修复方案。

3.8 安全事件响应

受多方面客观因素的影响，如产品自身的脆弱性不可能完全消除，外部威胁也在不断发展变化，当安全风险转变为安全事件时，就需要及时有效地进行安全响应，并与客户和其他利益相关方开展合作，确保快速安全地把系统恢复到期望的状态，以减少安全事件的不利影响。浪潮遵循国际安全事件/漏洞处理相关标准（如ISO/IEC 29147、ISO/IEC 30111），建立了完善的产品安全事件响应流程（如图3-8所示），确保产品漏洞信息得到及时披露，以及提供有效的产品漏洞修复解决方案。



图3-8 产品安全应急响应流程

在整个流程中，浪潮产品安全事件响应团队（Product Security Incident Response Team, PSIRT）负责接收、处理和披露产品相关安全漏洞和安全事件，并与外部第三方进行积极合作，以提高安全应急响应的效率。



浪潮产品安全应急响应流程包括4个阶段：

漏洞识别与接受

主要涉及漏洞主动监控与识别，以及内外部漏洞通知的接收。一方面我们成立了专门的安全团队负责主动监控互联网的安全漏洞发展情况，识别出对产品有影响的安全漏洞。另外一方面由PSIRT团队接收来自内外部与产品相关的安全事件和漏洞通知，包括客户、内部人员、供应商、外部安全团队或个人。我们鼓励负责任的漏洞披露，即外部漏洞发现者在公开披露前，应给予供应商一段合理的时间来解决相关问题。

供应商间高效的漏洞信息共享、公开透明的合作可有效缩短漏洞修复的时间，为此，我们也要求上游供应商主动与我们共享漏洞信息，并具备安全事件的响应能力，我们已经将这些要求作为协议/合同的一部分确保得到有效的履行。

分析验证

我们认真对待每个与产品相关的安全漏洞，无论是疑似的还是已经确认并公开的。PSIRT团队都与产品管理团队、产品研发团队、专业安全团队进行合作，快速启动分析调查工作，并依据CVSSv3³标准针对漏洞进行评估，确定漏洞等级。此阶段PSIRT团队会与漏洞通知者、第三方安全组织保持沟通，提高漏洞分析验证的真实性和及时性。

此外，我们会将已确认的安全漏洞录入产品安全漏洞库，对安全漏洞的修复进行全程跟踪和监控，确保这些安全漏洞得到有效的处理。

方案开发

一旦确认了漏洞存在，受影响的PDT/LMT团队将与内部专业安全团队协作，快速启动响应机制，对漏洞产生的根因，受影响的产品型号/版本范围进行评估。响应团队将根据漏洞风险程度来制定修复方案，包括临时规避方案、补丁包升级、版本升级等等。为确认这些方案的有效性，测试团队将对修复方案进行验证。

披露

在上述修复方案可用后，我们会及时通过官网安全公告、邮件及其他方式向漏洞报告者、客户、公众和其他利益相关方披露漏洞信息和修复方案信息。同时，我们也将积极跟踪客户对修复方案实施的有效性，确保修复方案的有效性。

为确保尽可能减少安全漏洞对客户的影响，针对每起安全漏洞事件，我们都将组织复盘会，分析问题原因和改进的措施。这些措施包括流程执行的效率，开发活动安全控制点的优化，代码安全检查点更新等等。通过复盘，持续提升产品安全能力，改进安全事件响应的效率。

3. <https://www.first.org/cvss/specification-document>

3.9 组织安全能力保障

3.9.1 信息安全

浪潮遵从ISO/IEC 27001建立信息安全管理体系，依照ISO/IEC 27002制定信息安全控制策略，定期进行内部审计、第三方机构的安全认证和审计来监督体系运行和持续改进。目前，浪潮的信息安全管理体系已通过ISO/IEC 27001认证。

在业务流程方面，浪潮将信息安全保障活动融入到供应链、产品研发、市场与销售、产品交付等各环节中，通过管理制度和技术规范来确保其有效实施。

在人员管理方面，浪潮的全体员工及合作伙伴都需严格执行公司的信息安全政策，签署保密协议，接受相关的安全培训，增强安全意识，提高安全技能，明确安全职责，以将安全方针和理念融入整个组织之中。对于违反信息安全政策的员工，浪潮将视情节严重程度给予处罚。

在风险管理方面，浪潮建立了风险评估管理规范，定期或根据重大变更执行安全风险评估，并进行有效的风险处置。

在业务连续性方面，浪潮规划业务连续性策略，制定和实施业务连续性计划，并通过应急预案演练对连续性计划的有效性进行验证。

3.9.2 个人隐私保护

公司高度重视隐私保护工作，遵守相关法律法规和监管机构的要求，积极探索个人隐私保护，建立个人信息保护框架，切实推行个人信息保护管理，为个人信息提供有效和可靠的保障，提高客户信任度。

公司遵守《通用数据保护条例》（GDPR）、《中国网络安全法》等各个国家和地区的相关法律法规和监管机构的要求，依据ISO/IEC 27701、ISO/IEC 29151和ISO/IEC 27001标准，及业界信息安全管理最佳实践，建立个人信息保护管理体系，并顺利通过ISO/IEC 27701隐私管理体系认证。

公司不断优化产品设计研发、生产交付、营销及运维服务等业务流程，基于隐私合规、数据最小化、公开透明等个人信息保护原则，采用合适的安全技术和控制手段，合理合法收集和處理客户、用户和员工的个人信息，确保个人信息主体行使有意义的、知情的、明确的、自由的同意权和选择权。

公司设立了个人信息保护部门（或隐私保护官），任何疑问、意见或建议可以通过发送邮件至lcxxsecurity@inspur.com的方式与其联系。



3.9.3 安全赋能培训

在全员信息安全意识和能力培训的基础上，我们还对涉及产品安全的重要岗位持续开展网络安全意识、知识和技能的培训，以便让他们能充分有效地履行岗位职责。我们针对不同岗位制定了针对性的安全能力提升计划和课程，通过系统地学习方案来提升员工的网络安全技能。同时，我们还鼓励员工积极参与内外部网络安全认证，从任职资格、绩效考核等方面牵引员工主动学习。目前，我们已有多人获得国际注册信息系统安全认证专家（CISSP）、注册信息安全专业人员（CISP）、注册信息安全渗透测试专家（CISP-PTS）等第三方专业安全认证。

3.9.4 内部审计/审核

公司建立了完善的内部审计/审核制度并执行定期审计，依据相关信息安全制度和流程规范，对各级组织及项目的安全活动合规性进行审计/审核等，出具审计/审核/评价意见等；针对内部审计/审核等发现的不符合项和待改进项，对应管理部门将跟踪并监督责任部门纠正或改进，确保各级管理体系健全有效。针对发现的重大缺陷，管理部门将根据有关制度，追究相关责任单位或者责任人的责任。



4 未来展望

美国著名科幻作家威廉·吉布森（William Gibson）曾说过“未来早已来到，只是尚未均匀分布”⁴。

以云计算、大数据、人工智能、物联网等新技术为代表的数字化时代已经来临，并在未来几年将持续影响全球经济社会的发展。我们比过去任何时候都更加重视保护个人隐私和组织数据，以及支撑经济社会发展和人民生活的关键信息基础设施。

但是我们可投入的资源总是有限，而我们面临的网络安全威胁和风险却是无限的。面对未来更多不确定因素和挑战，我们应如何前进？

我们认为公开、透明、互信的沟通与合作是应对问题和挑战的基础，因为在经济全球化的今天，没有哪一个组织可以解决如此复杂的问题。

我们将继续秉承开放、透明的方式，与监管机构、客户和其他利益相关方的开展沟通和合作，推动持续改进端到端的产品安全保障体系的完备性，确保我们的产品和服务符合相关法律法规和标准的要求。我们也将会继续坚持技术创新，投入更多资源进行安全技术和方法的研究，增强产品应对安全威胁的能力和韧性，尽可能减少安全风险带来的不利影响，以便能为客户持续提供安全可靠的产品和服务。

4. https://en.wikipedia.org/wiki/William_Gibson



5 关于浪潮信息

浪潮电子信息产业股份有限公司作为全球智慧计算的领先者，为云计算、大数据、人工智能提供领先的智慧计算。通过不断完善基于客户需求的服务器软硬件研发体系，公司目前已形成具有自主知识产权、涵盖高中低端各类型服务器、海量存储、云操作系统、信息安全技术的云计算IaaS层系列产品，为云计算IaaS层提供计算力平台支撑。公司在服务器、AI计算、开放计算、云等新兴应用处于全球领先地位，其中服务器销量全球前三、中国第一，增速全球第一，浪潮云服务器、人工智能服务器全球第一，浪潮存储全球第五，浪潮云操作系统中国前三。

公司聚焦人工智能和云计算变革发展机遇，全面升级智慧计算战略，充分利用并发挥在云数据中心核心装备和整体解决方案以及AI计算平台的领先优势，坚持“开放、融合、敏捷”策略，以实现“引领信息科技浪潮，推动社会文明进步”为目标，以“创新”赢未来，构建全球化的智慧计算生态，成为全球领先的全栈式智慧计算方案供应商。

多年来，浪潮始终践行开放计算的理念，引领开放计算的标准，是全球唯一的三大开放组织发起成员或白金会员，牵头了服务器全部国标，是OpenStack黄金会员，社区贡献中国第一，同时还连续2年担任全球SPECML技术委员会主席。持续定义领先的开放计算产品，拥有全球唯一符合三大开放标准组织的整机柜产品，拥有全球架构最全、配置最多、规格最高的开放计算服务器，最先开发了开放技术的OAM加速计算模块和OTII边缘计算服务器，拥有全球性能领先的存储系统等。

inspur 浪潮

激活智慧计算

版权声明

Copyright©2021浪潮电子信息产业股份有限公司版权所有。您可以为内部参考的目的复制和使用本文档。本文档未授予任何其他许可。

商标声明

inspur 浪潮 inspur 是浪潮集团有限公司的注册商标。本文档提及的所有其他公司的名称和商标，由其各自所有者拥有。

责任声明

本文档按“原样”提供，不作任何明示或暗示的保证。任何保证均明确予以否认，包括但不限于不侵权、商用性以及特定目适用性的保证。

本文档仅供参考使用，浪潮不保证所呈现信息的精确性。本文档提供的任何信息可能会被纠正、修改和改变，恕不另行通知。

任何使用或信赖本文档所提供信息的风险自行承担。



www.inspur.com