

# T/JXEA

## 江西省工程师联合会团体标准

T/JXEA 363—2026

### 计算机系统智能安全防护规程

Technical specifications for intelligent security protection of computer systems

(征求意见稿)

2026—XX—XX 发布

2026—XX—XX 实施

江西省工程师联合会 发布

## 目 次

前 言 .....	错误！未定义书签。
引 言 .....	III
1 范围 .....	1
2 规范性引用文件 .....	1
3 定义 .....	1
4 安全防护体系架构与建设原则 .....	2
5 身份鉴别与访问控制管理 .....	2
6 智能监测与入侵防御技术规范 .....	2
7 数据安全与隐私保护技术 .....	3
8 安全审计与日志管理技术规范 .....	3
9 应急响应与灾难恢复技术规范 .....	3
10 运维管理与人员安全要求 .....	4

## 前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由XXX提出。

本文件由XXX归口。

本文件起草单位：

本文件主要起草人：

## 引 言

随着信息技术的快速发展，计算机系统已成为支撑社会运行的关键基础设施。然而，网络攻击手段日益智能化、隐蔽化，传统的被动防御体系已难以应对复杂多变的安全威胁。建立一套集主动防御、智能感知、动态响应于一体的计算机系统安全防护规程，是保障国家关键信息基础设施安全、维护数据主权和个人隐私的迫切需求。

本规程重点涵盖了从基础环境安全、身份访问控制，到基于人工智能的威胁监测、数据加密保护，以及应急响应与灾备恢复等核心环节。本规范旨在填补智能化安全防护技术标准的空白，推动信息安全建设从合规性向实效性的转变。

本规程的实施，将有助于构建“全域感知、智能协同、主动防御”的新型安全体系，为数字中国建设提供坚实可靠的技术支撑与制度保障。

# 计算机系统智能安全防护规程

## 1 范围

本文件规定了计算机系统智能安全防护的体系架构、身份鉴别、智能监测、数据安全、安全审计、应急响应以及运维管理等方面的技术要求和管理规范。

本文件适用于指导各类计算机系统（包括服务器、终端、网络设备及应用系统）的安全规划、建设、运维及测评工作，是构建智能化安全防护体系的依据。涉及国家秘密的计算机系统，还应符合国家保密法律法规和标准的要求。

## 2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 22240 信息安全技术 网络安全等级保护定级指南

GB/T 25069 信息安全技术 术语

GB/T 35273 信息安全技术 个人信息安全规范

GM/T 0054 信息系统密码应用基本要求

NY/T 1213 农作物种子标签和使用说明技术规范

## 3 术语和定义

下列定义适用于本文件。

### 3.1

**智能安全防护** intelligent security protection

利用人工智能、大数据分析等技术，对计算机系统中的安全数据进行采集、分析与挖掘，实现对潜在威胁的自动识别、预警、阻断及响应的主动防御机制。

### 3.2

**零信任架构** zero trust architecture

一种以“持续验证、永不信任”为核心原则的安全模型。在该模型中，无论网络流量源自内部还是外部，都必须经过严格的身份认证和授权才能访问系统资源。

### 3.3

**安全态势感知** security situation awareness

基于环境的、动态的、整体地洞悉安全风险的能力。利用大数据分析技术，从全局视角提升对安全威胁的发现、预警和响应处置能力。

### 3.4

**数据脱敏** data desensitization

对某些敏感信息通过脱敏规则进行数据的变形，实现对敏感隐私数据的可靠保护，同时保留数据的原有业务属性和特征，以满足开发测试等非生产环境的需求。

### 3.5

**蜜罐技术** honeypot technology

一种诱骗防御技术。通过构建包含漏洞的虚假系统或服务，诱导攻击者进行攻击，从而收集攻击者的工具、策略和意图信息，为防御体系提供情报支持。

### 3.6

#### 灾难恢复 disaster recovery

为了将信息系统从灾难造成的故障或瘫痪状态恢复到可正常运行状态、并将支持的业务功能从灾难造成的不正常状态恢复到可接受状态，而设计的活动和流程。

## 4 安全防护体系架构与建设原则

计算机系统智能安全防护体系的建设应遵循"纵深防御、主动免疫、智能协同"的原则，构建涵盖物理环境、网络通信、区域边界、计算环境及应用业务的多维防护架构。具体而言，应依据GB/T 22239的相关规定，按照业务系统的功能、重要性及安全等级，对网络进行逻辑或物理的隔离划分，核心业务区、管理区、对外服务区之间应部署防火墙、网闸等访问控制设备，严格限制跨区域的非授权访问；针对云计算环境，应建立虚拟化安全防护机制，确保虚拟机之间的隔离性，对虚拟化管理平台实施严格的访问控制和审计，防止虚拟机逃逸等高级威胁；应部署统一的安全信息和事件管理

（SIEM）平台，汇聚防火墙、入侵检测系统（IDS）、终端检测与响应（EDR）等各类安全设备的日志数据，利用机器学习算法，对海量日志进行关联分析，实现对未知威胁的快速发现与精准定位；系统架构设计应具备自我修复能力，当检测到核心组件遭受攻击或故障时，能自动切换至备用节点或降级运行模式，确保关键业务不中断；系统建设完成后，应参照GB/T 22240进行等级保护定级，并定期开展风险评估和渗透测试，及时发现并修补架构层面的安全隐患。

## 5 身份鉴别与访问控制管理

### 5.1 身份鉴别要求

身份鉴别是计算机系统安全的第一道防线，应采用高强度的身份认证机制，确保用户身份的真实性和唯一性。系统应支持基于数字证书、动态口令、生物特征（指纹、虹膜等）的多因素认证

（MFA）技术，严禁仅使用单一的静态口令作为高敏感系统的登录凭证；对于特权账号（如系统管理员、数据库管理员），应实施严格的审批和授权流程，特权操作必须经过二次认证，并实时记录操作全过程。

### 5.2 访问控制策略

访问控制策略应遵循最小权限原则（Principle of Least Privilege），即用户仅被授予完成其工作所必需的最小权限。应建立基于角色的访问控制（RBAC）模型，根据用户的角色动态分配权限，避免权限滥用；在零信任架构下，每一次访问请求都必须经过身份验证和授权决策引擎的实时评估。应利用SDP（软件定义边界）技术，实现"先认证，后连接"，隐藏内部应用系统，防止网络扫描和资产暴露。

## 6 智能监测与入侵防御技术规范

### 6.1 网络流量监测

智能监测与入侵防御系统应具备对网络流量、主机行为、应用日志的实时分析能力，利用人工智能技术识别异常行为和未知威胁。网络流量监测应部署具备深度包检测（DPI）能力的探针，对进出网络边界的数据包进行全流量分析。利用AI算法建立业务流量基线模型，当检测到流量突增、协议异常或特征码匹配（如已知病毒库、木马特征）时，系统应自动触发告警并阻断恶意连接。

### 6.2 主机安全防护

主机层面应部署EDR（终端检测与响应）系统，持续监控终端的进程行为、注册表修改、文件操作等。一旦发现勒索软件加密行为、挖矿程序启动等恶意活动，应立即隔离受感染终端并清除威胁。

### 6.3 高级威胁防御

针对高级持续性威胁（APT），应引入蜜罐技术和沙箱技术。蜜罐用于诱捕攻击者，沙箱用于对可疑文件进行动态行为分析。通过将分析结果同步至防火墙和WAF（Web应用防火墙），实现全网防御策略的联动更新。

## 6.4 自动化响应

防御系统应具备自动化编排与响应（SOAR）能力。当检测到大规模DDoS攻击或蠕虫病毒传播时，系统应自动执行预定义的剧本（Playbook），如自动调整防火墙策略、切断攻击源IP、隔离受感染网段等，将响应时间缩短至分钟级。

## 7 数据安全与隐私保护技术

### 7.1 数据采集与传输

数据是计算机系统的核心资产，必须采取加密、脱敏、备份等多种技术手段，保障数据在采集、传输、存储、使用、共享及销毁全生命周期的安全。数据采集应符合GB/T 35273的规定，遵循合法、正当、必要的原则。对于个人信息的收集，必须获得用户的明确授权，并采取加密传输通道，防止数据在采集端被窃取；数据传输过程中，应利用SSL/TLS、IPSec或国密算法（SM2/SM3/SM4）对传输通道进行加密。对于跨网络边界的敏感数据传输，必须经过网闸的严格过滤和审计。

### 7.2 数据存储与加密

数据存储应实施分类分级保护。核心数据和重要数据应采用高强度加密算法进行存储加密。密钥管理应符合GM/T 0054的要求，使用经国家密码管理局认证的密码机或密钥管理系统（KMS）进行密钥的生成、存储和分发。

### 7.3 数据使用与销毁

数据使用与共享环节，应采用数据脱敏技术，对敏感字段（如身份证号、手机号、银行卡号）进行掩码处理。对于开发测试环境，严禁使用未经脱敏的真实生产数据；数据销毁应采用符合国家标准的数据擦除工具，对存储介质上的数据进行不可逆的覆写清除，确保数据无法被恢复。

## 8 安全审计与日志管理技术规范

### 8.1 日志记录要求

安全审计是追溯安全事件、分析攻击路径的重要手段，系统应具备完善的日志记录和审计分析能力。计算机系统应开启全面的审计功能，记录用户登录、权限变更、配置修改、数据访问、策略调整等关键操作日志。日志内容应包含操作时间、操作主体（用户/设备）、操作对象、操作结果等关键信息。

### 8.2 日志存储与保护

日志记录应具备防篡改特性。应采用WORM（一次写入多次读取）存储技术或区块链存证技术，确保日志一旦生成便不可被修改或删除；日志应集中存储于专用的日志服务器或SIEM平台，存储期限应符合国家法律法规要求，且不少于180天。

### 8.3 审计分析与报告

审计分析系统应具备关联分析能力。通过将网络层日志、主机层日志和应用层日志进行关联，还原攻击者的完整攻击链。对于高风险操作（如特权账号登录、核心数据批量导出），系统应实时触发告警并通知安全管理员；应定期生成安全审计报告。报告内容应涵盖系统运行状态、安全事件统计、漏洞修复情况、策略有效性评估等，为管理层提供安全决策依据。

## 9 应急响应与灾难恢复技术规范

### 9.1 应急响应机制

计算机系统应建立完善的应急响应机制和灾难恢复体系，确保在遭受重大安全事件或自然灾害后，能够迅速恢复业务运行。组织应建立网络安全应急响应小组（CERT），制定详细的应急预案。预案应涵盖病毒爆发、网络攻击、数据泄露、硬件故障等各类场景，并明确各岗位的职责和处置流程。

### 9.2 应急演练与容灾备份

建立常态化的应急演练机制。每年至少组织一次全要素的应急演练，包括桌面推演和实战攻防演练，检验应急预案的有效性，提升人员的应急处置能力；关键业务系统应建立异地容灾备份中心。依据GB/T 20988《信息安全技术 信息系统灾难恢复规范》的要求，核心业务数据应实现实时或准实时的异地同步，确保在主中心发生灾难时，备中心能够接管业务。

### 9.3 应急物资与复盘分析

建立应急物资储备库，储备必要的备品备件（如服务器、交换机、防火墙等）和应急工具箱。在发生硬件故障时，能够快速进行替换和修复；安全事件处置结束后，应进行复盘分析。总结经验教训，完善防护策略，修补系统漏洞，并形成事件处置报告归档保存。

## 10 运维管理与人员安全要求

### 10.1 人员资质与轮岗

运维管理是计算机系统安全运行的保障，应建立严格的管理制度，规范人员行为，降低内部风险。运维人员应实行持证上岗制度，具备相应的专业技术能力和安全保密意识。关键岗位应实施轮岗和强制休假制度，防止因人员长期在同一岗位而产生的道德风险。

### 10.2 运维操作审批

建立严格的运维操作审批流程。对于高危操作（如系统重装、数据删除、核心配置修改），必须经过书面审批，并在非业务高峰期由双人复核后执行。

### 10.3 运维审计与培训

运维审计（堡垒机）应作为唯一的运维入口。所有运维操作必须通过堡垒机进行，实现对运维会话的全程录像和指令级审计，确保操作行为可追溯；加强人员安全意识培训。定期开展网络安全法律法规、典型案例和防范技能的培训，每年不少于两次，提高全员对钓鱼邮件、社交工程等攻击手段的识别能力。

### 10.4 保密协议管理

签订保密协议。所有接触核心数据和系统权限的人员，必须签订保密协议，明确保密义务和法律责任，离职时应立即收回所有权限并进行安全审计。

---