ICS 35.020
L 01
备案号：46310-2015

DB32

江　苏　省　地　方　标　准

DB32/T 2776-2015

生态环境监控系统建设规范 安全体系

Specifications for construction of ecological environment monitoring system
Security system

2015-06-15 发布　　2015-08-15 实施

江苏省质量技术监督局　　发 布

目　　次

前言 III
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 通用安全要求 2
4.1 物理安全 2
4.2 网络安全 3
4.3 主机与数据库安全 4
4.4 安全审计 5
5 计算域安全要求 6
5.1 计算域的分类 6
5.2 互联网计算域 6
5.3 内联网计算域 9
6 边界安全要求 11
6.1 边界的划分 11
6.2 互联网出口边界 12
6.3 互联网服务器边界 13
6.4 互联网内联边界 13
6.5 内联网服务器边界 13
6.6 数据中心边界 13
6.7 外联网边界 13
7 系统建设安全要求 14
7.1 安全方案设计 14
7.2 产品采购和使用 14
7.3 自行软件开发 14
7.4 外包软件开发 14
7.5 工程实施 14
8 安全过程 15
8.1 流程图 15
8.2 安全策略 15
8.3 安全保护 16
8.4 安全检测 16
8.5 事件响应 16
8.6 系统恢复 17

9 常规安全管理 17
9.1 机房环境管理 17
9.2 资产管理 17
9.3 设备管理 17
9.4 安全事件管理 18
9.5 网络安全管理 18
9.6 系统安全管理 18
9.7 变更管理 18
10 安全产品使用 18
附 录 A （规范性附录） 信息安全策略表 20
附 录 B （规范性附录） 安全产品使用作用 22

前　言

本标准按照GB/T 1.1—2009的规定编制。

本标准由江苏省环境保护厅提出并归口。

本标准起草单位：江苏省生态环境监控中心、江苏省标准化研究院、江苏天创科技有限公司。

本标准主要起草人：李军、刘珏、何春银、刘清、徐益强、许萌君、陈媛、徐洁、吴杰、寇晓芳。

生态环境监控系统建设规范　安全体系

1　范围

本标准规定了生态环境监控系统建设中通用安全要求、计算域安全要求、边界安全要求、系统建设安全要求、安全过程、常规安全管理和安全产品使用 。

本标准适用于生态环境监控系统建设中信息系统安全建设、安全运维、安全等级测评和风险评估等。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 18336.1-2009　信息技术 安全技术 信息技术安全性评估准则 第1部分:简介和一般模型

GB/T 22239-2008　信息安全技术信息系统安全等级保护基本要求

GB/T 25069-2010　信息安全技术 术语

GB/Z 20986-2007　信息安全技术 信息安全事件分类分级指南

3　术语和定义

GB/T 18336.1-2009、GB/T 25069-2010界定的以及下列术语和定义适用于本文件。

3.1

信息系统　information system

由计算机、网络、及各种软件组成，在特定的工作平台上完成数据的传输、处理、查寻、存储等工作任务。

[GB/Z 20986-2007,定义 2.1]

3.2

计算域　computational domain

由数据安全存储、传输和处理的计算环境组成的区域。

注：安全计算域根据应用安全需求划分，可以由单一安全计算机系统如安全数据服务器、安全终端计算机等组成，也可以由多个安全计算机系统经安全通信网络连接组成。

3.3

安全边界　safety limits

系统软件中不同区域间进行数据传输的关口。

3.4

内联网 intranet

支持各部门或机构进行业务处理和信息交流的网络信息系统。

3.5

数据计算域 data computing domain

提供数据处理、传输、存储的平台。

3.6

服务计算域 services computing domain

终端计算机提供信息录入、检索、发布等的服务平台。

3.7

终端计算域 terminal computing domain

使用信息系统的作用主体，向系统发出服务请求。

4 通用安全要求

4.1 物理安全

4.1.1 物理位置的选择

4.1.1.1 机房应选择在具有防震、防风和防雨等能力的建筑内。

4.1.1.2 机房场地不应设在建筑物的高层或地下室，以及用水设备的周边或隔壁。

4.1.1.3 机房不应设在有强电磁环境干扰、加油站等高危险场所的一公里以内。

4.1.2 物理访问控制

4.1.2.1 机房入口和重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员信息。

4.1.2.2 应对机房划分物理区域进行管理，物理区域之间设置物理隔离装置。

4.1.3 防盗窃和防破坏

4.1.3.1 应将主要设备放置在机房内。

4.1.3.2 应将主要部件进行固定，并设置明显的不易除去的标记。

4.1.3.3 应将通信线缆铺设在隐蔽处，可铺设在地下或管道中。

4.1.3.4 应对介质分类标识，存储在介质库，重要资料应存放档案室中。

4.1.3.5 应利用光、电等技术设置机房防盗报警系统。

4.1.3.6 应对机房设置监控报警系统。

4.1.4 防雷击

4.1.4.1 机房建筑应设置避雷装置。

4.1.4.2 应设置防雷保安器，防止感应雷。

4.1.4.3 机房应设置交流电源地线。

4.1.5 防火

4.1.5.1 机房应设置面向电子设备的火灾自动消防系统，实现自动检测火情、自动报警，并自动灭火。

4.1.5.2 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。

4.1.5.3 机房应采取区域隔离防火措施，将重要设备与其他设备隔离开。

4.1.6 防水和防潮

4.1.6.1 水管安装，不得穿过机房屋顶和活动地板下。

4.1.6.2 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。

4.1.6.3 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。

4.1.6.4 应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。

4.1.7 防静电

4.1.7.1 主要设备与机柜应采用必要的接地防静电措施。

4.1.7.2 机房应采用防静电地板。

4.1.8 温湿度控制

机房应设置温、湿度自动调节设施，并部署温、温度自动监控、报警装置。

4.1.9 电力供应

4.1.9.1 应在机房供电线路上配置稳压器和过电压防护设备。

4.1.9.2 应提供短期的备用电力供应，至少满足主要设备在断电情况下的正常运行要求。

4.1.9.3 应设置冗余或并行的电力电缆线路为计算机系统供电。

4.1.10 电磁防护

4.1.10.1 应采用接地方式防止外界电磁干扰和设备寄生耦合干扰。

4.1.10.2 电源线和通信线缆应隔离铺设，避免互相干扰。

4.1.10.3 应对关键设备和磁介质实施电磁屏蔽。

4.2 网络安全

4.2.1 网络结构安全

4.2.1.1 主要网络设备的业务处理能力应具备冗余空间，满足业务高峰期需要。

4.2.1.2 应保证网络各个部分的带宽满足业务高峰期需要。

4.2.1.3 应在业务终端与生态监控系统之间进行路由控制建立安全的访问路径。

4.2.1.4 应绘制与当前运行情况相符的网络拓扑结构图。

4.2.1.5 应根据生态环境监控系统的业务关系划分区域，为各区域分配独立的子网或网段，区域间应采用可靠的技术隔离手段。

4.2.1.6 应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段。

4.2.1.7 应按照对生态监控系统服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护业务应用的带宽。

4.2.2 网络设备身份鉴别

4.2.2.1 应对登录网络设备的用户进行身份鉴别。

4.2.2.2 身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求与定期更换要求。

4.2.2.3 应具有登录失败响应功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施。

4.2.2.4 应设置连接超时功能，超时后自动中断连接。

4.2.2.5 当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被获取。

4.2.2.6 应对网络设备的管理员登录地址进行限制。

4.2.2.7 应定期检查并锁定或撤销不必要的账号。

4.2.3 网络设备防护

4.2.3.1 应定期对网络设备的配置文件进行备份，配置发生变更时应及时备份原有配置。

4.2.3.2 应定期对网络设备运行状况进行检查。

4.2.3.3 应关闭网络设备上不使用的端口，并建立相应的端口开放审批制度。

4.2.3.4 应定期检验网络设备软件版本信息，避免使用软件版本中出现的安全隐患。

4.2.3.5 网络设备用户的标识应具有唯一性。

4.2.3.6 应实现设备管理员、操作员、审计员的权限分离。

4.3 主机与数据库安全

4.3.1 主机与数据库身份鉴别

主机身份鉴别应符合5.2.3的规定。

4.3.2 主机与数据库访问控制

4.3.2.1 应依据工作权限最小化原则启用访问控制功能。

4.3.2.2 应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限。

4.3.2.3 应实现操作系统和数据库系统特权用户的权限分离。

4.3.2.4 应严格限制默认帐户的访问权限，重命名系统默认帐户，修改默认帐户的默认口令。

4.3.2.5 应及时锁定或撤销多余的、过期的帐户，避免共享帐户的存在。

4.3.3 主机与数据库剩余信息保护

4.3.3.1 应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除。

4.3.3.2 应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。

4.3.4 主机入侵防范

4.3.4.1 应能对重要程序的完整性进行检测，并具有完整性受到破坏后的恢复措施。

4.3.4.2 操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。

4.3.4.3 操作系统开放的服务应遵循小化原则，关闭系统运行时不需要的应用服务。

4.3.5 主机恶意代码防范

4.3.5.1 应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库。

4.3.5.2 主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库。

4.3.5.3 应支持防恶意代码的统一管理。

4.3.6 主机与数据库资源控制

4.3.6.1 应通过设定终端接入方式、网络地址范围等条件限制终端登录。

4.3.6.2 应根据安全策略设置登录终端的操作超时锁定。

4.3.6.3 应对重要服务器进行监视，包括监视服务器的 CPU、硬盘、内存、网络等资源的使用情况。

4.3.6.4 应限制单个用户对系统资源的最大或最小使用限度。

4.3.6.5 应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。

4.3.7 软件安全

4.3.7.1 应部署全网用户的软件资源库，为用户提供常用软件下载安装。

4.3.7.2 应软件或软件版本更新前，应有专人对软件进行检测，通过审批后方可将新软件向用户发布。

4.3.7.3 应部署相应技术手段控制终端用户通过非法途径获得的软件或非授权的软件在终端计算机上进行安装。

4.3.7.4 生产系统服务器安装新软件需通过相关的授权审批。

4.4 安全审计

4.4.1 网络安全审计

4.4.1.1 应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录，内容包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

4.4.1.2 应对网络中产生的正常通信内容进行梳理，并制定非正常通信内部的监测预警策略，及时将网络中非正常的通信内容采取技术手段通知安全管理人员。

4.4.1.3 应能够根据记录数据进行分析生成审计报表。对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。

4.4.2 主机安全审计

4.4.2.1 审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户。

4.4.2.2 审计内容包括：重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件。

4.4.2.3 审计记录应包括：事件的日期、时间、类型、主体标识、客体标识和结果等。

4.4.2.4　能根据记录数据进行分析，并生成审计报表，应保护审计进程，避免受到未预期的中断，应保护审计记录，避免受到未预期的删除、修改或覆盖等。

4.4.3　应用安全审计

4.4.3.1　应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计，审计记录至少包括：事件的日期、时间、发起者信息、类型、描述和结果等。

4.4.3.2　应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录，应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

5　计算域安全要求

5.1　计算域的分类

根据业务安全需求可划分为两个计算机域：互联网计算域与内联网计算域。在两个计算域中根据业务应用关系可划分多个子域，见图1。

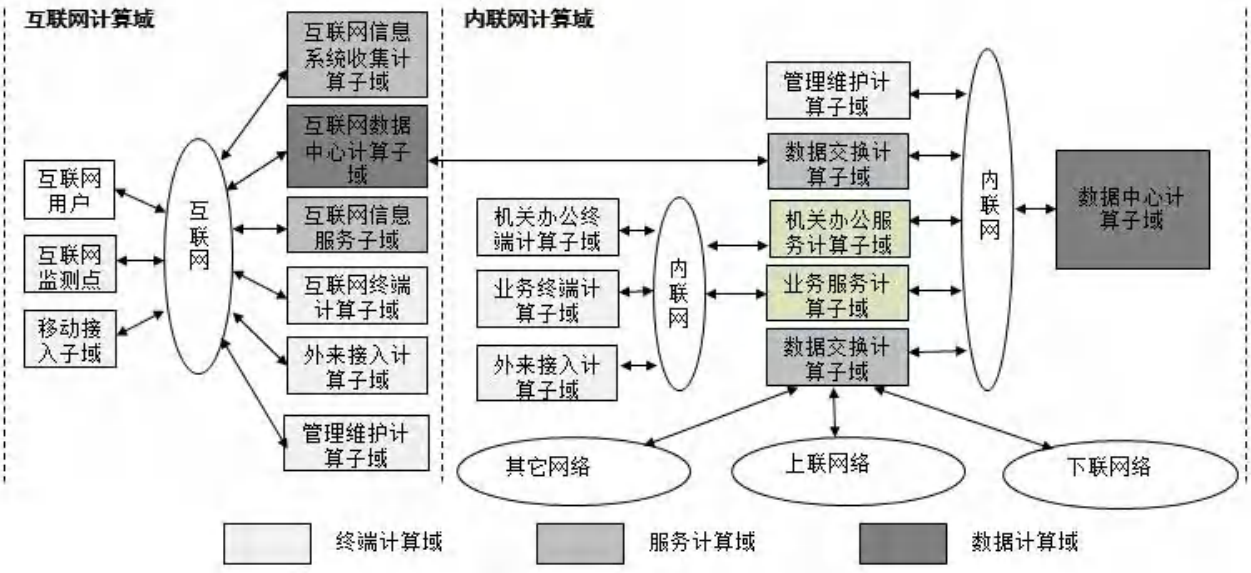

图1　安全计算域划分图

5.2　互联网计算域

5.2.1　互联网信息服务计算子域

5.2.1.1　公共信息服务类

5.2.1.1.1　应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问。

5.2.1.1.2　访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作。

5.2.1.1.3　应由授权主体配置访问控制策略，并严格限制默认帐户的访问权限。

5.2.1.1.4　应授予不同管理帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。

5.2.1.1.5　应具有对重要信息资源设置敏感标记的功能。

5.2.1.1.6　应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

5.2.1.1.7 应定期或在应用文件发生变更时备份系统文件，备份文件应场外存储。

5.2.1.1.8 应部署防篡改技术，防止主要的网站页面被恶意篡改。

5.2.1.2 非公共信息服务类

5.2.1.2.1 应符合 5.2.1.1.1 规定。

5.2.1.2.2 具备应用身份鉴别的功能，应实现：

——提供专用的登录控制模块对登录用户进行身份标识和鉴别，并使用两种及以上的组织鉴别技术；

——提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；

——提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

——启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

5.2.1.2.3 应采用密码技术保证通信过程中数据的完整性。

5.2.1.2.4 具备通信保密性，应实现：

——在通信双方建立连接之前，应用系统利用密码技术进行会话初始化验证；

——对通信过程中的整个报文或会话过程进行加密。

5.2.1.2.5 具备抗抵赖的功能，应实现：

——具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能；

——具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能。

5.2.1.2.6 具备软件容错，应实现：

——提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求；

——提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。

5.2.1.2.7 具备应用资源控制，应实现：

——当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方能够自动结束会话；

——能够对系统的最大并发会话连接数进行限制；

——能够对单个帐户的多重并发会话进行限制；

——能够对一个时间段内可能的并发会话连接数进行限制；

——能够对一个访问帐户或一个请求进程占用的资源分配最大限额和最小限额；

——能够对系统服务水平降低到预先规定的最小值进行检测和报警；

——提供服务优先级设定功能，并在安装后根据安全策略设定访问帐户或请求进程的优先级，根据优先级分配系统资源。

5.2.1.2.8 具备应用剩余信息保护，应实现：

——保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；

——保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。

5.2.2 互联网信息收集计算子域

互联网信息收集计算域安全应符合5.2.1.1.1的规定：

5.2.3 互联网终端计算机子域

5.2.3.1 主机身份鉴别

5.2.3.1.1 应对终端计算机登录操作系统用户进行身份标识和鉴别。

5.2.3.1.2 操作系统身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换。

5.2.3.2 主机访问控制

5.2.3.2.1 应限制终端计算机用户通过管理员账号登录计算机。

5.2.3.2.2 应严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令。

5.2.3.2.3 应及时删除多余的、过期的帐户，避免共享帐户的存在。

5.2.3.2.4 应限制在终端计算机上处理及存放机关办公文件及业务工作文件。

5.2.3.3 主机入侵防范

5.2.3.3.1 终端计算机操作系统应启用个人防火墙功能，限制其它计算机访问终端计算机。

5.2.3.3.2 终端计算机操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序。

5.2.3.3.3 应通过统一的补丁服务器更新终端计算机的系统补丁。

5.2.3.4 主机恶意代码防范

5.2.3.4.1 应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库。

5.2.3.4.2 主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库。

5.2.3.4.3 应支持防恶意代码的统一管理。

5.2.4 管理维护计算机子域

5.2.4.1 主机身份鉴别

身份鉴别的安全要求应符合5.2.3.1的规定。

5.2.4.2 主机访问控制

管理维护计算机域的访问控制除应符合5.2.3.2的规定外，还应实现：

——限制外来计算机接入或访问管理维护计算域。

——限制管理维护计算域的计算机不能连接互联网。

5.2.4.3 主机入侵防范

入侵防范的安全要求应符合5.2.3.3的规定。

5.2.4.4 主机恶意代码防范

恶意代码防范的安全要求应符合5.2.3.4的规定。

5.2.5 外来接入计算机子域

5.2.5.1 入网身份鉴别

5.2.5.1.1 应为已获得授权的外来计算机分配接入本计算域的账号与口令。

5.2.5.1.2 应限制已获得授权的外来计算机接入本计算域的时间，超时后自动锁定账号。

5.2.5.2 网络访问控制

应限制已获得授权的外来计算机的访问范围。

5.2.6 移动接入子域

5.2.6.1 主机身份鉴别

身份鉴别的安全要求应符合5.2.3.1的规定。

5.2.6.2 主机访问控制

5.2.6.2.1 应限制终端计算机用户通过管理员账号登录计算机。

5.2.6.2.2 应严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令。

5.2.6.2.3 应及时删除多余的、过期的帐户，避免共享帐户的存在。

5.2.6.3 主机入侵防范

5.2.6.3.1 终端计算机操作系统应启用个人防火墙功能，限制其它计算机访问终端计算机。

5.2.6.3.2 终端计算机操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序。

5.2.6.3.3 应及时更新终端计算机的系统补丁。

5.2.6.4 主机恶意代码防范

应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库。

5.2.6.5 通信安全

通过互联网连接到内部网络时应采取有效的通信加密措施，加密强度不低于128位。应中断与互联网的其它接连，采取双因子的认证方式并控制访问的范围。

5.2.7 互联网数据中心计算子域

5.2.7.1 数据完整性

应能够检测到系统管理数据、鉴别信息和重要业务数据在传输与存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。

5.2.7.2 备份和恢复

5.2.7.2.1 应提供本地数据备份与恢复功能，完全数据备份至少每天一次，备份介质应场外存放。

5.2.7.2.2 应提供异地数据备份功能，利用通信网络将关键数据定时批量传送至备用场地。

5.2.7.2.3 应采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障。

5.2.7.2.4 应提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性。

5.3 内联网计算域

5.3.1 数据中心计算子域

数据中心计算子域的安全保护要求应合5.2.7的规定。