互联网数据中心（IDC）网络安全管理的设计与应用

刘伟

中国电信股份有限公司河北分公司，河北石家庄，050000；

摘要：在当前信息技术飞速发展背景下，互联网数据中心（IDC）已成为支撑数字时代发展的关键基础设施。IDC 承载大量企业和个人的数据，由此其网络安全管理的重要性不言而喻。基于此，本文研究中将深入探究 IDC 安全管理系统构建路径，针对其技术框架、软件结构以及功能模块等设计思路进行分析，以此为保障信息安全提供必要支持。

关键词：互联网数据中心；网络安全；管理

DOI：10.69979/3041-0673.24.9.004

引言

互联网数据中心（IDC）在实际发展中主要承担互联网服务提供商、企业以及政府机构存储、处理和分发数据的核心职能，其安全状况直接对网络生态系统整体稳定性以及数据资产安全性造成影响。在当前云计算、大数据、物联网等技术得到广泛应用背景下，IDC 所承载数据量以及业务复杂度也日益增加，此不仅会带来巨大的商业价值，同时也使得 IDC 成为网络攻击者主要目标。因此，构建出高效、可靠且可扩展的网络安全管理体系，对保障 IDC 的运行正常性以及数据安全性具有至关重要的影响。在具体开展 IDC 网络安全管理体系设计时，需要对多种因素进行综合考量，具体内容包括但不限于物理安全、网络安全、主机安全、应用安全和数据安全等。其中，物理安全主要是为保障数据中心物理设施不受破坏；网络安全则主要关注防御外部网络攻击以及内部网络异常行为；主机安全主要倾向服务器以及终端设备安全防护；应用安全则主要关注应用程序漏洞以及安全缺陷；数据安全则主要涉及数据加密、备份以及恢复等。

1 系统技术框架及软件体系设计要点

1.1 技术框架

IDC 管理系统实际构建过程中，其存在多元化实施路径，系统核心架构如图 1 所示，由图中信息可知，系统主要由两大核心控制组件构成：中心指挥单元（CCU）以及行动执行单元（AEU）。其中 CCU 主要承担指令集散地职能，不仅接收来自管理层（用户）的指令并对数据进行反馈，同时还需承担 AEU 集群调度以及管理工作，具体内容涵盖指令的分配、传递执行及数据的整合分析，同时可在必要情况下触发预警机制。系统基础架构主要覆盖用户服务托管、综合管控平台、应用服务支撑层及网络资源共享区等关键元素。

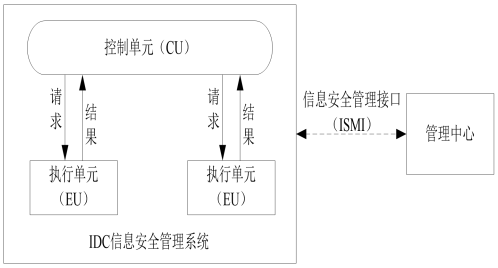

图 1 IDC 实现方式示意图

1.2 软件架构设计要点

IDC 信息安全管理系统在实际开发过程中，主要采用成熟且可靠的软件架构范式，整体架构可被划分为用户交互界面层、业务逻辑处理层以及数据管理与访问层，其具体布局如图 2 所示。

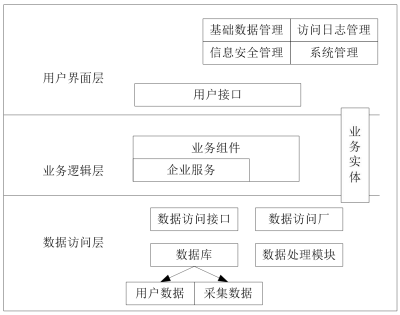

图 2 系统体系架构

用户界面层：该层为架构顶层，其中集成有丰富的交互元素以及直观的操作界面。该层在实际运行中主要基于多样化的交互组件库，以切实提升用户操作灵活性。同时，界面设计对安全访问控制进行重点强调，其中主要涵盖登录验证以及安全主操作界面，以保障仅授权用户可对系统进行访问，并有效执行管理任务。

业务逻辑层：该层主要承担系统核心处理中枢职责，主要负责 IDC 管理系统相关业务逻辑的运算以及执行，其功能与计算机系统中的 CPU 较为类似，该层对系统流

畅性以及响应速度具有重要影响，其可有效保障系统运行高效性。

数据访问层：该层主要作为数据管理核心区域，其重点集中在数据资源存取控制、优化管理及安全防护。该层除负责数据传输、存储职能外，还涉及数据修正、完善以及优化工作，以最优方式促进数据在系统内的流通，以此构建出保障数据完整性以及安全性的坚固防线。

通过上述优化设计，IDC 管理系统可有效实现架构清晰分层、功能明确划分以及高效协同作业，进而为系统稳定运作与后续持续优化升级奠定坚实的基础。

2 系统功能模块设计要点

2.1 基础数据管理模块设计要点

IDC 信息安全管理体系核心在于构建出多元化数据架构，其主要通过对多种数据类型进行集成并切实强化操作后的即时反馈机制，以保障所有数据变更以及操作记录均可被迅速、安全地传达到监控核心，以此为深入分析提供相应数据基础支持。该模块可赋予安全监管层全面的控制权，以有效实现对基础数据进行高效、灵活管理目标。尤其是在机房 IP 环境监控方面，其构建出较为严密的防护网，可精准捕捉未经授权访问、异常行为及潜在威胁模式，对关键信息（如 IP 地址、访问路径、异常行为特征、用途及时间戳等）进行详细记录，同时在信息在规定周期内进行有效上报，以此维护系统状态实时同步与查询效率的高效性。

2.2 访问日志模块设计要点

该模块主要聚焦于网络流量以及访问日志的一体化管理方面。一方面，该模块可依托于精准追踪 IDC 上行流量，对用户访问轨迹进行详细描绘，以此生成详尽的访问日志，此可大幅提升安全监管查询效率；另一方面，该模块在实际运行中可有效强化日志统计功能，具体运行中可充分围绕 IP 地址、访问时段等核心维度开展深度剖析，同时该模块针对 HTTP 协议增设 URL 保留机制，可有效满足复杂多变的查询与统计需求，支持时间、IP、URL 等多条件灵活组合查询。

2.3 信息安全管理模块设计

IDC 信息安全管理系统中的信息安全管理模块可被细化为三大核心组件，以实现强化网络环境纯净度与合规性目标，相关组件主要包括违规站点管控、不良信息监测与判定以及非法信息拦截与净化机制，其具体职能阐述如下：

第一，违规站点综合治理模块。该模块主要承担甄别并初步应对互联网数据中心（IDC）中存在的违法违规网站职能。该模块不仅可对不合规站点进行即时检测，同时还可执行初步分析处理措施，并详尽记录相关关键信息，如注册域名、IP 分配、违规手法等。此外，该模块还可对处理状态（如已实施干预或待处理）进行标记，同时记录操作账户信息及时间戳，以此保障各环节均可追溯。相关数据可依托于定时机制向安全监管平台同步，以此为监管方查证与复核提供便利条件支持。

第二，不良信息智能监测与记录模块。该模块主要用于对 IDC 中流转的不良信息进行捕捉，若识别出相应信息则立即开展初步净化，并生成详尽的监测日志。相关日志不仅会对不良信息发现过程进行详细记录，同时还可有效保障信息可迅速传递给后端的安全监管体系，以便开展更深入的分析与处理。依托于该机制，可切实缩短从发现到响应的时间链，进而提升整体防控效率。

第三，非法信息动态过滤与日志上报引擎。针对 IDC 双向数据流中的异常数据，该引擎可有效实施精密监控与即时过滤策略。若检测到不符合安全标准的数据流，系统将立即启动过滤程序，同时生成涵盖源/目的 IP 地址、代理行为等关键信息的过滤日志。相关日志不仅可对过滤操作进行全面记录，同时也可为后续分析与优化过滤规则提供重要依据支持。随后，相关经过整理的过滤日志可被即时提交至安全监管系统，并辅助其制定或调整基于 IP、域名、URL、关键词等多维度的过滤策略，以此进一步增强网络安全屏障稳固性。

其具体作业流程图如图 3 所示。

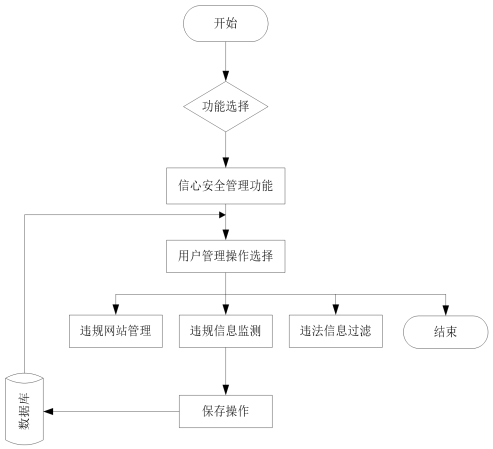

图 3 信息安全管理功能流程图

2.4 系统接口设计要点

2.4.1 命令通道

该系统在实际设计中创新性地构建出基于 WebService 的指令传输框架，作为核心通信手段，进而充分实现管理中心与信息安全管理体系间实现无缝指令对接。管理中心在实际运行中可动态地发起请求，并利用专门设计的接口方法（如 idc_command）方法），将管理意

图以 XML 格式进行封装，同时通过 WebService 将其高效传输至信息安全管理系统之中。此机制可赋予管理中心灵活调控系统基础监控功能的能力，同时可为信息安全状态及配置表深度分析与适时调整提供必要支持。指令流转具体逻辑如下：（1）指令发起与封装。管理中心首先发出指令请求，随后将指令内容编译为标准化的 XML 文档，在此基础上依托于 WebService 通道进行发送；（2）接收与双重验证。信息安全管理系统在完成指令接收后，即开始执行身份与数据完整性双重核验工作。在验证无误后，对指令进行记录并准备反馈执行状态，无论操作成败均向管理中心进行报告；若接收遇阻，则管理中心相应依据反馈采取重发措施；（3）执行与应答。验证通过指令将按时执行，同时依托于 idc_commandack() 机制，将执行结果迅速回传至管理中心之中；（4）数据交互附加操作。若指令涉及数据处理相关内容，则系统将自动触发数据上报流程，以此保障数据流转合规性。

2.4.2 数据通道

为切实强化系统内部模块的数据透明性以及实时性，该系统在实际规划设计中编织出严密的数据上报流程，其主要依托 SMMS 为各 ISMS 分配独特的 IDC/ISP 根目录，进而实现数据集中化管理与高效流通。数据交互关键环节如下：

（1）数据预处理与封装。ISMS 在实际开展数据传输作业前，需将数据转化为 XML 格式，随后依托于 file_load 函数开展压缩加密，切实提升数据传输安全性以及效率。

（2）验证与数据恢复。SMMS 在完成数据接收后，会立即执行详尽的验证流程，具体内容主要涵盖安全校验和身份确认，以保障数据源准确无误。验证成功后，数据将被解压缩、解密，以此为后续处理奠定坚实基础。

（3）数据处理与存储。该流程主要依据预设处理逻辑，对验证后的数据开展相应操作，并将处理结果以适宜格式储存于系统之中，以此为后续信息检索与分析提供便利条件支持。

（4）结果反馈机制。在完成上述操作后，ISMS 可主动请求获取操作结果文档，并通过解析结果文件，对操作有效性和准确性进行评估，以此保障数据整体上报流程的闭环性和可靠性。

3 系统功能测试

为验证本文所研究 IDC 信息安全管理系统功能成效，技术人员在实际工作中对基础数据管理功能、访问日志管理模块以及信息安全管理模式进行试验验证。

3.1 基础数据管理功能测试

对该功能模块进行性能测试时，主要需对数据查询、数据监测以及数据管理三方面进行测试，具体结果如表 1 所示。

表 1 系统基础数据管理模块测试结果

测试功能	序号	使用人员	测试类型	测试过程	测试过程	预期结果	实际结果
查询功能	1-1	用户	UI 界面	核对界面字体和按钮配置准确性	目测法	界面良好	正常
	1-2		控件测试	验证控件在未输入数据状态下的正常运作	任意操作控件	系统正常	正常
	1-3		功能测试	获取经营单位、客户、IP 地址、域名及链路相关数据	输入查询信息名称并点击确认	系统可显示对应信息	正常
	1-4				输入不存在信息名称并点击确认	所显示数据为空	正常
数据监测功能	2-1	用户	UI 界面	核对界面字体和按钮配置准确性	目测法	界面良好	正常
	2-2		控件测试	验证控件在未输入数据状态下的正常运作	任意操作控件	系统正常	正常
	2-3		功能测试	系统是否可对基础数据信息进行监测	点击监控按钮	系统可实时显示相应数据	一般缺陷，数据过长情况下无显示
数据管理功能	3-1	用户	UI 界面	核对界面字体和按钮配置准确性	目测法	界面良好	正常
	3-2		控件测试	验证控件在未输入数据状态下的正常运作	任意操作控件	系统正常	正常
	3-3		功能测试	用户添加信息	输入信息并点击添加	可正常增添信息	正常
	3-4			用户删除信息	选中信息并选择删除	可正常删除信息	正常
	3-5			用户修改信息	选中信息并选择修改	可正常修改信息	正常
	3-6			用户查询信息	输入查询信息后触发按钮确认	可正常显示查询信息	正常

3.2 访问日志管理模块测试

对该功能模块进行性能测试时，主要需对查询以及源目 IP 查询功能进行测试，具体结果如表 2 所示。

表 2 访问日志管理模块功能测试结果

测试功能	序号	使用人员	测试类型	测试过程	测试过程	预期结果	实际结果
查询功能	4-1	用户	UI 界面	核对界面字体和按钮配置准确性	目测法	界面良好	轻缺陷，查询界面字体存在差异
	4-2		控件测试	点击查询	在不输入信息情况下点击查询	显示出查询结果	正常
	4-3				在输入查询目标情况下点击查询	显示出查询结果	正常
	4-4		功能测试	对用户登录以及访问信息进行查询	输入用户 IP 并进行查询	正常显示查询结果	正常
源目 IP 查询功能	5-1	用户	UI 界面	核对界面字体和按钮配置准确性	目测法	界面良好	正常
	5-2		控件测试	点击源目 IP 查询按键	不输入信息进行查询	显示出查询结果	正常
	5-3				输入信息进行查询	显示出查询结果	正常
	5-4		功能测试	依据输入的源目 IP 对信息进行查询	输入源目 IP 并查询	正常显示查询结果	正常

3.3 信息安全管理模块测试

对该功能模块进行性能测试时，需主要针对违法违规网站管理、违法信息监测以及违法信息过滤功能进行测试，结果如表 3 所示。

表 3 违法违规网站管理功能测试结果

序号	使用人员	测试类型	测试过程	测试过程	预期结果	实际结果
6-1	用户	UI 界面	核对界面字体和按钮配置准确性	目测法	界面良好	正常
6-2		控件测试	验证控件在未输入数据状态下的正常运作	任意操作控件	系统正常	正常
6-3		功能测试	对违法违规网站监控进行记录	点击网站监控	实时显示监控数据	正常
6-4			依照危险等级采取预设处理措施	存在违规网站时点击分析按钮	依据违规等级选择相应处理方法	正常
6-5			数据上报安全监管系统	点击违规上报功能	信息成功上报	严重缺陷，信息上报错误

4 总结

综上所述，通过对本文所研究 IDC 信息安全管理系统功能进行测试分析，可知，该系统大部分功能均可正常运行，仅发现轻缺陷、一般缺陷以及严重缺陷各一个，其余功能均可正常运行，由此其具备较强应用价值。

参考文献

[1]孙智.互联网数据中心(IDC)云计算在通信领域中的应用与安全风险研究[J].长江信息通信,2023,36(8):222-224.
[2]高轶浪.IDC 互联网数据中心信息安全与应对措施[J].数字化用户,2021(51):70-72.
[3]韩普,周北望,金石.陕西广电网络数据中心设计方案[J].网络安全和信息化,2020(8):5.
[4]张靖韬.IDC 网络安全常见问题与应对策略研究[J].通讯世界,2021,028(007):57-58.
[5]李跃华.互联网数据中心(IDC)的互联网接入方案分析[J].电子世界,2021,(017):47-48.
[6]石晶.IDC 机房 IT 支撑平台软件运维管理子系统[J].网络安全技术与应用,2020(8):2.
[7]孙海华.5G 商业化应用下的互联网+IDC 发展趋势研究[J].中国商论,2020(8):2.