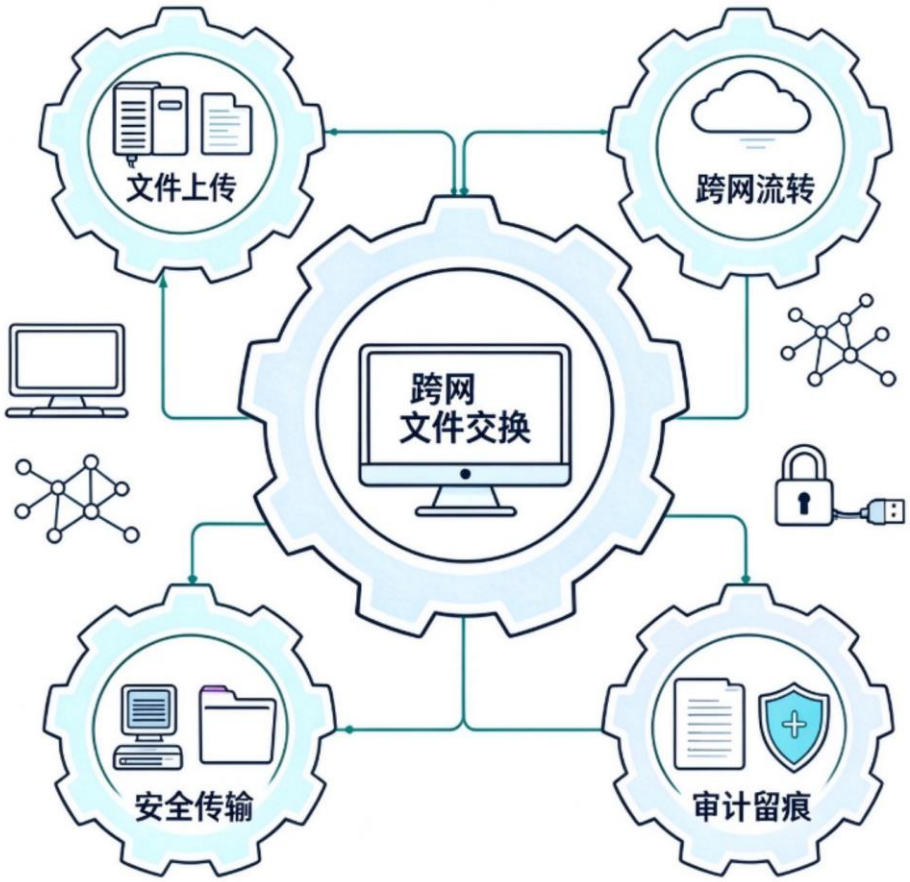
域智盾软件®

域智盾跨网
文件交换系统白皮书

White Paper on Cross-Network File Exchange System



河北中视新研软件开发有限公司

CONTENTS 目录

修订记录.....4
序　言.....5
一、关键发现.....5
1.1 企业面临的真实困境.....5
1.2 文件跨网交换趋势.....6
1.3 面临的挑战.....7
1.4 大致解决思路.....8
二、跨网文件交换典型场景.....8
三、方案概述.....9
3.1 定义.....9
3.2 网络拓扑.....9
3.3 产品结构与功能体系.....10
四、管理员用户手册.....10
4.1 全局搜索.....11
4.2 文件列表.....11
4.2.1 我的文件.....11
4.2.2 网络区域文件.....11
4.3 我的分享.....12
4.4 审批管理.....12
4.4.1 流程模板.....13
4.4.2 审批任务.....13
4.4.3 外部通知管理.....13
4.5 策略管理.....13
4.6 日志.....14
4.6.1 文件管理日志.....14
4.6.2 文件分享日志.....14
4.6.3 病毒查杀日志.....14
4.6.4 申请记录日志.....15
4.6.5 任务处理日志.....15
4.7 组织架构管理.....15
4.8 系统管理.....15
4.8.1 系统配置.....16
4.8.2 网卡配置.....16
4.8.3 病毒库升级.....16
4.8.4 准入联动管理.....17
4.8.5 系统授权.....17
4.8.6 系统状态.....17
五、用户操作手册.....18
5.1 登录账户.....18
5.2 核心功能.....19
5.2.1 我的上传.....19

5.2.2 分享给我.....19
5.2.3 群文件.....20
5.2.4 我的分享.....21
5.2.5 审批任务.....21
六、代表企业.....22
七、资质与荣誉.....22
八、实践案例.....23
九、未来安全趋势展望.....24
版权说明.....25
免责声明.....25

修订记录

本白皮书随产品版本迭代与用户实践更新，修订情况记录如下。

版本	修订日期	修订内容	编制
V1.0	2026 年 11 月	首次发布。确立跨网文件交换的需求框架、典型场景、系统定义与能力框架，编制管理员手册与用户手册的功能说明，并给出实施路径与案例。	域智盾软件运营部

序　言

网络分域隔离，是我国网络安全等级保护制度、涉密信息系统分级保护要求以及行业监管规范共同确立的基本原则。办公网与互联网之间、涉密网与非涉密网之间、生产控制网与管理网之间、研发网与办公网之间，原则上不建立直接连通，这一原则在制度层面已经相当成熟。

现实中，一份合同需要发给客户，一张图纸需要交给供应商，一份检测报告需要报送主管部门，一段视频素材需要从互联网侧导入剪辑系统。这些需求有一个共同特征——传递行为发生在制度之外，既没有申请，也没有审批，更没有记录。

因此，跨网文件交换要解决的不是“能不能传”的问题，而是“能不能按规矩传”的问题。规矩包括四件事：谁申请、谁批准、传了什么、传到哪里。这四件事在纸面上都写清楚了，缺的是承载它们的系统。

本白皮书讨论的正是这一层：把跨网文件交换从个人行为转为组织行为，从物理摆渡转为系统流转，从口头同意转为审批留痕。

全书结构如下。

第一章给出关键发现，包括企业真实困境、交换趋势、面临挑战与解决思路；

第二章按六类典型场景说明不同网络环境下的交换要求；

第三章给出系统定义与能力框架；

第四章从管理员视角说明功能构成；

第五章从使用者视角说明功能构成；

第六章介绍代表企业；

第七章列示资质；

第八章为脱敏案例；

第九章对未来趋势作出判断。

一、关键发现

1.1 企业面临的真实困境

在对多个行业用户的实施前调研中，跨网文件交换环节暴露出以下 5 类共性问题。

- 传递手段原始：U 盘、移动硬盘、光盘刻录仍是主要方式，介质在多人之间流转，来源与去向无法确认，一旦涉入病毒或敏感文件，追责缺少依据。
- 审批停留在纸面：多数单位设有《跨网数据交换审批单》，但审批单与文件本身不绑定，审批通过后传了什么、传了几份、是否与申请一致，无人核对。
- 日志靠人工登记：交换记录由经办人手工填写台账，填写随意、更新滞后，检查时难以自证。
- 涉敏内容无审查：文件是否含敏感词、是否含个人信息、是否属于禁止外发范围，完全依赖经办人判断，缺少一致性标准。
- 责任边界模糊：文件由谁上传、谁审批、谁下载，分散在不同环节，出现问题时无法形成完整链条。



图 1-1 企业面临的真实困境

1.2 文件跨网交换趋势

从近三年的项目实践看，跨网交换正在发生五个方向的变化。

- 隔离要求在强化，而非放松

等级保护测评对边界防护的要求逐年细化，涉密网与互联网之间的物理隔离检查趋严，工控网络与办公网络之间的横向连通被明确限制。

- 交换量在增长，而非减少

设计与仿真文件体积持续增大，单份图纸从数十兆升至数百兆；检测报告、影像资料、视频素材的批量交换成为常态。以介质手工摆渡的方式，在数据量面前已经不可持续。

- 审批在线上化

纸质审批单逐步被线上流程替代，与办公平台、企业微信、钉钉的对接成为基本要求。

- 留痕成为刚性要求

监管检查、内审、客户审计均要求提供完整的交换记录，包括申请理由、审批人、文件清单、检查结果、下载记录，仅能提供汇总台账已不满足要求。

- 交换系统从“通道”变为“平台”

早期产品只解决文件搬运，当前需求已扩展到权限、策略、审查、配额、日志、联动，交换系统正在成为企业跨域数据流转的基础设施。

1.3 面临的挑战

- 安全与效率的平衡：检查环节越多，传递越慢，若一次交换需要半天，使用者必然回到U盘。
- 大文件与批量场景：数百兆的设计文件、上千个文件的批量导入，对传输稳定性、断点续传、进度可见提出要求，普通网页上传方式难以承载。
- 双向与多域结构：一次交换可能涉及内网、外网、专网、合作方网络四个域，系统需要支持多网络区域的定义与区域间策略，而不是只做两点之间。
- 检查能力需内嵌：病毒查杀与涉敏审查若作为独立环节，使用者在流程之外自行处理，等于没有检查。
- 权限颗粒度：既要按部门授权，也要按网络区域授权，还要按单个账户授权，临时项目组、外部合作方需要临时权限，到期须自动收回。
- 审计可读性：日志若只是流水记录，检查人员无法使用，系统需要把日志组织成可检索、可导出、可对应的证据材料。

1.4 大致解决思路

针对上述挑战，本产品的解决思路可归纳为五条原则。

1. 独立通道：以专用系统承载跨网交换，系统独立部署、独立授权、独立审计，不与办公系统混用。
2. 审批前置：文件在上传后即进入审批流程，未获批准不得进入目标网络区域。
3. 检查内嵌：病毒查杀与涉敏审查作为流程节点自动执行，检查结果作为审批依据呈现给审批人，未通过检查的文件不进入下一环节。
4. 全程留痕：申请、审批、检查、上传、下载、分享、删除七类动作全部记录，记录与文件、账户、网络区域关联，可按任一维度检索。
5. 最小授权：按网络区域、部门、账户三级授权，默认不可见、按需开放、到期收回，管理员操作本身亦受限制并留痕。

二、跨网文件交换典型场景

不同网络环境的交换目的、频率与敏感程度差异明显，系统在同一套框架下按场景配置不同策略。以下六类场景来自实际项目，覆盖多数用户的主要需求。

场景	主要方向	核心风险	策略要点
办公网-互联网	资料导入、材料外发	病毒进入、内部文件外流	双网登录、病毒查杀、外发审批
涉密网-非涉密网	参考导入、材料导出	涉密信息失控	多级审批、涉敏审查、水印与有效期
生产网-办公网	工艺下发、数据回传	生产中断、参数外泄	固定目录、专用账户、免客户端接入
研发网-办公网	资料获取、成果评审	代码与图纸外泄	项目分区、评审模板、批量下载提醒
总部-分支	制度下发、业务报送	权限越界、口径不一	多区域结构、分级审批、分级查看
企业-合作方	交付物发送、资料接收	外部扩散、责任不清	临时账户、分享有效

期、提取码

图 1-2 跨网文件交换的典型场景

三、方案概述

3.1 定义

域智盾跨网文件交换系统，是部署于网络边界、用于在不同网络区域之间完成文件受控传递的软件系统。

系统的核心特征是三个“不”：

①动作不留白，七类操作全部记录；

②网络不直连，两个区域之间不存在 IP 层通路；

③人员不越界，账户与网络区域绑定，只能看到被授权的区域。

需要区分的是，本系统不替代防火墙、网闸等边界设备，也不承担网络层的隔离职责。它解决的是隔离前提下的文件流转问题：边界设备决定“两个网络能不能通”，本系统决定“哪些文件、经谁批准、以什么方式通过”。

3.2 网络拓扑

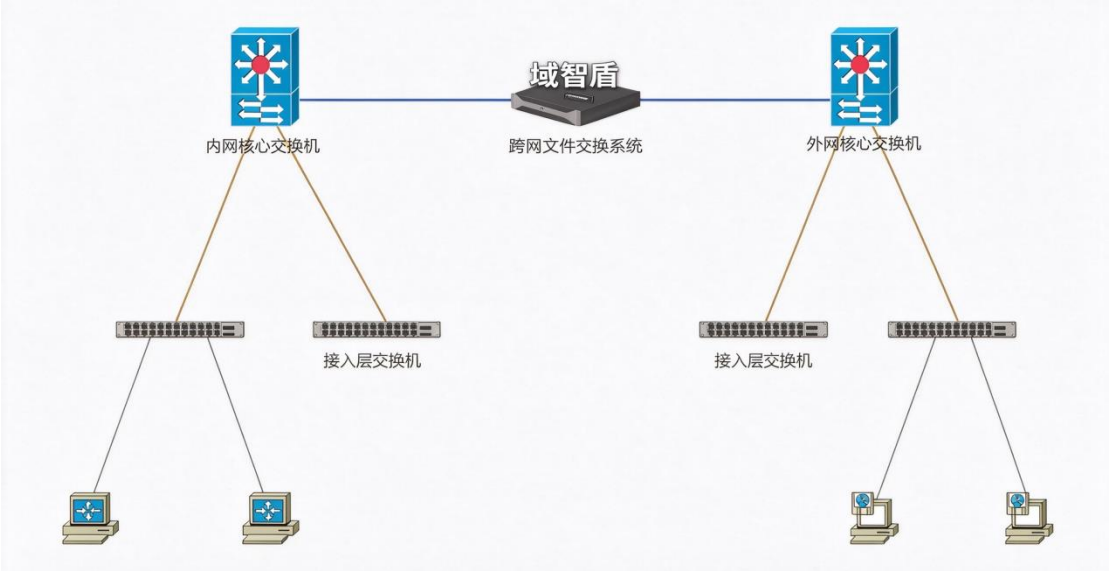


图 1-3 网络拓扑图

核心步骤：

①服务器断电状态下完成线缆连接，接线完成后再给服务器加电；

②将服务器 ETH0 网口接入内网核心交换机，其余网口分别对接其他网络的核心交换机；

③使用网线直连服务器 ETH3 网口与运维计算机；

④将运维计算机 IP 配置为同网段 1.2.3.3，子网掩码设置 255.255.255.0。

服务器各网口说明：

ETH0：系统管理网口，管理员通过连接 ETH0 网口 IP 地址登录系统管理平台。

ETH3：系统初始配置网口。（系统默认 IP 地址 1.2.3.4）

3.3 产品结构与功能体系



图 1-4 产品结构与功能体系

四、管理员用户手册

本章说明管理员侧的功能构成。

4.1 全局搜索

全局搜索面向跨网系统管理员，提供对全系统已上传文件的内容级检索能力。管理员在首页输入关键词即可检索所有账户上传的文件，检索范围覆盖文件名与文件内容，不受账户与部门归属限制，但检索行为本身记录在案。

检索结果以列表呈现文件的基本信息，包括文件名、文件大小、当前状态、上传时间、上传账户与所属网络区域。管理员可对命中文件执行下载并本地查看，用于核实文件内容是否与申请描述一致。

4.2 文件列表

文件列表分为“我的文件”与“网络区域文件”两个视图，前者面向管理员自身的上传，后者面向全网。

4.2.1 我的文件

该视图呈现当前账户（含管理员账户）上传文件的基本信息，包括文件名、文件大小、上传时间与当前状态。状态区分待审批、审批中、已批准、已拒绝、已过期、已删除等，使用者可据此判断文件所处环节。

视图内提供目录级操作能力：

- 支持新建目录、移动文件至指定目录、按目录层级浏览；
- 上传与下载过程显示进度，大文件传输中断后可续传；
- 对单个文件提供预览、下载、分享、删除与查看详细信息等操作。

详细信息包含文件属性、检查结果、审批记录与下载记录，是核实一次交换完整过程的最小单元。

4.2.2 网络区域文件

该视图按网络区域组织，呈现各区域已上传文件的基本信息，包括文件名、文件大小、上传时间、作者与当前状态。管理员可对各区域文件执行预览、下载、分享、删除与查看文件详情。

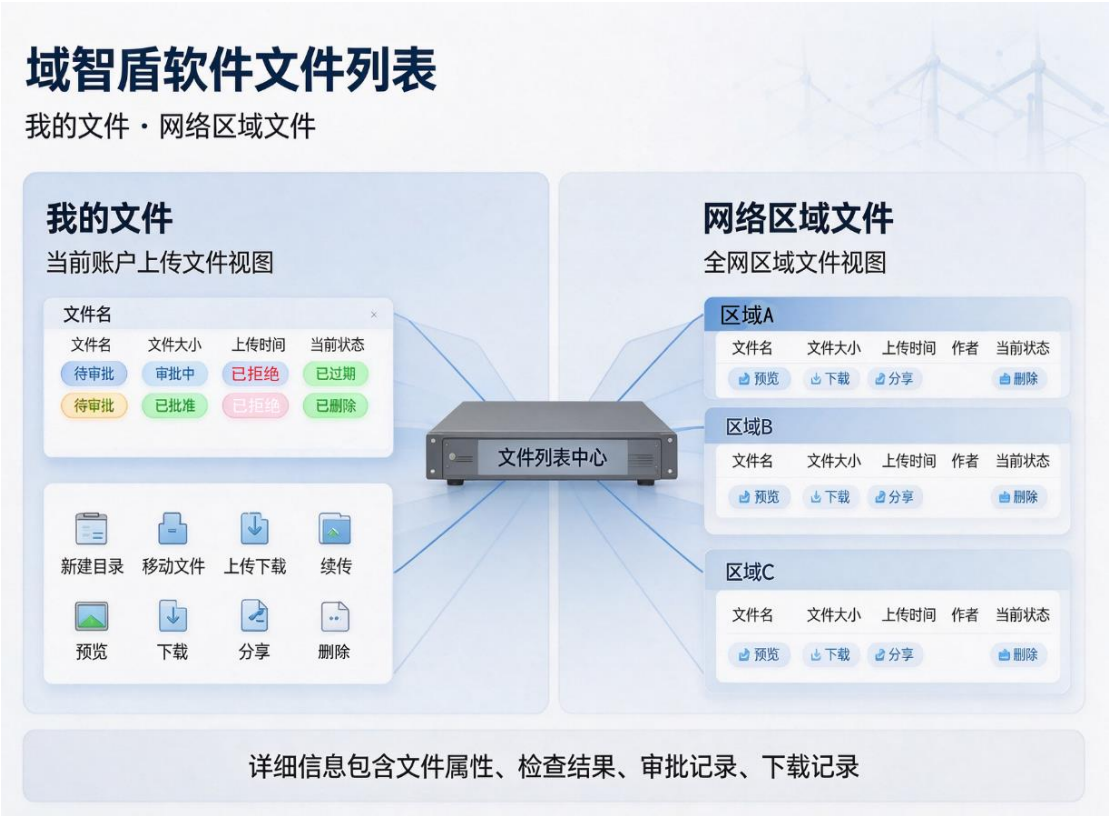


图 1-5 文件列表

4.3 我的分享

分享是跨网交换中使用频率最高的动作之一，也是外泄风险最集中的环节。该功能呈现当前账户已分享文件的信息，包括文件名、文件大小、分享于何时、有效时间与当前状态。

分享可设定有效期、提取码与下载次数上限，三项共同构成对外传递的边界：

- 有效期控制时间窗口；
- 提取码控制访问主体；
- 下载次数控制扩散范围。

效果：到期或次数用尽后链接自动失效，无需人工干预。

4.4 审批管理

审批管理由流程模板、审批任务、外部通知管理三部分构成。

4.4.1 流程模板

支持在文件上传至流转结束之间插入若干审批环节，每个环节可设定环节名称、审批人与审批模式。审批人可设定多名，支持按角色指定而非固定到人，人员变动时流程不受影响；审批模式分为严格与简单两种，严格模式要求全部审批人通过方可放行，简单模式任一人通过即可。

4.4.2 审批任务

审批任务视图汇总待处理与已处理的申请，呈现任务名、类型、当前状态、申请原因、提交时间与完成时间。审批人可在此查看申请文件详情、检查结果与申请人信息，据此作出批准或拒绝的判断，拒绝时须填写原因，原因回传至申请人。

任务按处理时限排序，超时任务突出显示，对同一申请人的同类高频申请，支持批量处理，减少重复劳动。

4.4.3 外部通知管理

外部通知管理用于与企业微信、钉钉进行绑定，完成账户关联配置与互联网路由设置后，申请与审批消息可推送至审批人日常使用的办公平台，实现“消息到人”。

绑定关系由管理员统一维护，员工离职或调岗时随账户状态自动失效。

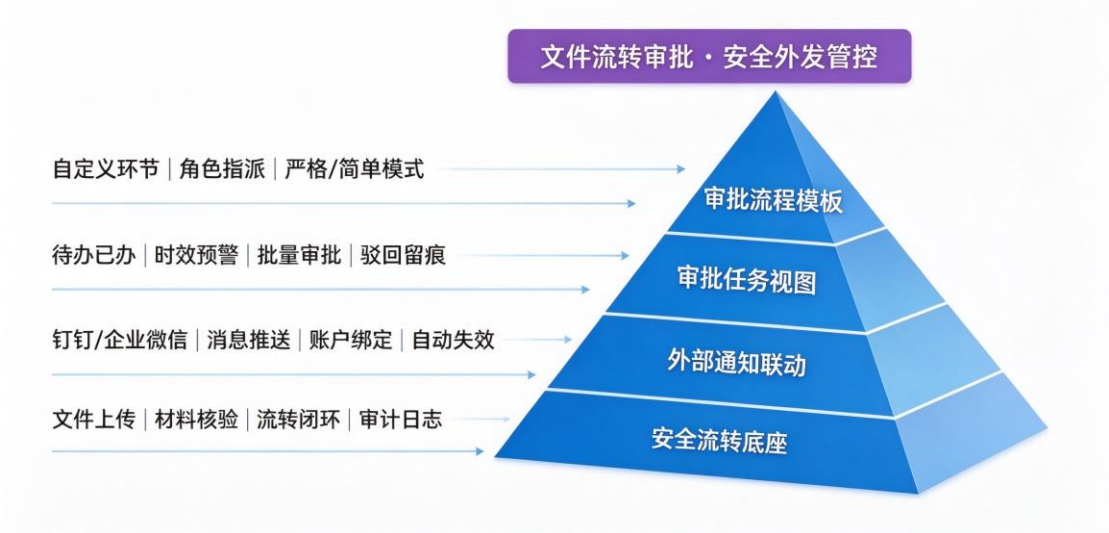


图 1-6 审批管理

4.5 策略管理

覆盖六类策略。

- 账户限制策略：规定上传频次、单次文件数量、单文件大小上限与可访问区域，防止个别账户成为不受约束的通道；
- 配额管理：为部门与账户设定存储上限，超出后禁止上传并提示清理；
- 文档类型策略：以扩展名白名单方式限定可交换范围，阻断可执行文件、脚本与特殊格式；
- 清理规则：设定文件保留天数，到期自动转入待清理区并按设定方式处理，避免存储写满；
- 涉敏检查：设定敏感词库与命中动作，可设置为仅提示、阻断或转人工复核；
- 人工审核：设定哪些操作须经管理员确认，如大文件导出、批量下载、跨区域移动。

4.6 日志

日志是系统对外提供证据的能力，共分五类，均支持删除与导出为 Excel 表格，导出保留原始字段，便于二次整理。

4.6.1 文件管理日志

记录全网文件的上传与流转，字段包括文件名、文件大小、所在工作区、操作者、操作类型、详情与时间。该日志回答“哪份文件、由谁、在什么时间、进入了哪个区域”，是核查交换行为的主干记录。

4.6.2 文件分享日志

记录分享类动作，字段包括文件名、文件大小、所在工作区、操作员、操作与时间。用于核查外发链条：某份文件是否被分享、分享给谁、是否被提取。

4.6.3 病毒查杀日志

记录每次检查的结果，字段包括文件名、文件大小、所在工作区、作者、病毒名称、病毒信

息与时间，检出记录独立留存，即便文件随后被删除，检查结论仍可查证。

4.6.4 申请记录日志

记录申请侧信息，字段包括申请名、申请人、事务类型、申请原因与处理时间。该日志的价值在于呈现“为什么传”——申请原因是审计判断合理性的关键依据。

4.6.5 任务处理日志

记录审批侧信息，字段包括任务名、处理人、处理结果、拒绝原因与处理时间。

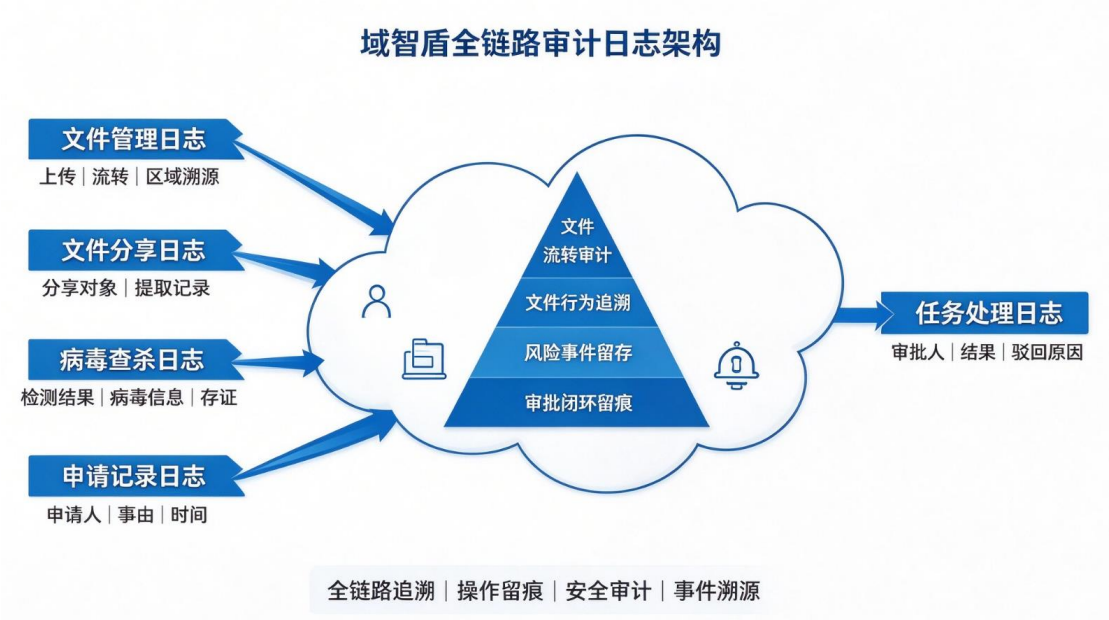


图 1-7 日志

4.7 组织架构管理

部门层级支持多级，人员归属到部门后自动继承部门策略，组织调整时，支持部门迁移与人员调岗，迁移过程保留历史记录，避免出现“人已调走、权限仍在”的情形。

4.8 系统管理

系统管理面向系统管理员，承担运行维护职责，包含六组功能。

4.8.1 系统配置

系统配置集中管理账户安全与运行参数：

- 密码错误尝试次数限制连续输错的最大次数；
- 锁定违规账户时长设定触发锁定后的禁止登录时间；
- 启用密码复杂度验证后，系统自行检测所设密码的复杂程度；
- 修改服务器时间用于校时；
- 服务器升级与客户端升级分别上传升级文件完成版本更新；
- 数据备份与还原支持导出系统数据或在需要时回传恢复；
- 重启服务器设备用于在维护窗口内重启服务。

4.8.2 网卡配置

网卡配置用于对服务器的 ETH0 网卡设定 IP 地址、子网掩码与网关，使系统接入管理网络。业务网口按网络区域分别配置，配置变更记录在案，便于排查“某区域无法访问”类问题。

4.8.3 病毒库升级

支持在线更新与离线导入两种方式，离线方式适用于不与互联网连通的部署环境，可由管理员定期从外部获取升级包后导入。病毒库版本与更新时间在界面可见，便于确认检查能力是否处于有效状态。



图 1-8 病毒库升级

4.8.4 准入联动管理

准入联动用于与网络准入系统协同。配置联动参数后，跨网交换的账户状态、设备合规状态可与准入系统相互校验：未通过准入校验的设备无法登录交换系统；交换系统中的违规记录可回传准入系统，作为后续准入判断的依据。这一联动把“交换”与“接入”两个环节的规则统一起来，避免出现“设备进不来、文件却能传出去”的缝隙。

4.8.5 系统授权

系统授权用于上传授权文件，激活已采购的授权范围，包括可管理的网络区域数量、账户数量与并发数。授权到期前系统提示续期，避免因授权失效导致交换中断。

4.8.6 系统状态

系统状态呈现三项运行指标：系统运行状态（各服务进程是否正常）、系统 CPU 占用状态、内存与磁盘占用情况。磁盘占用尤其需要关注——跨网交换系统长期运行会积累大量文件，磁盘写满将直接导致上传失败。系统状态与清理规则配合使用，可在容量接近阈值时提前处

理。

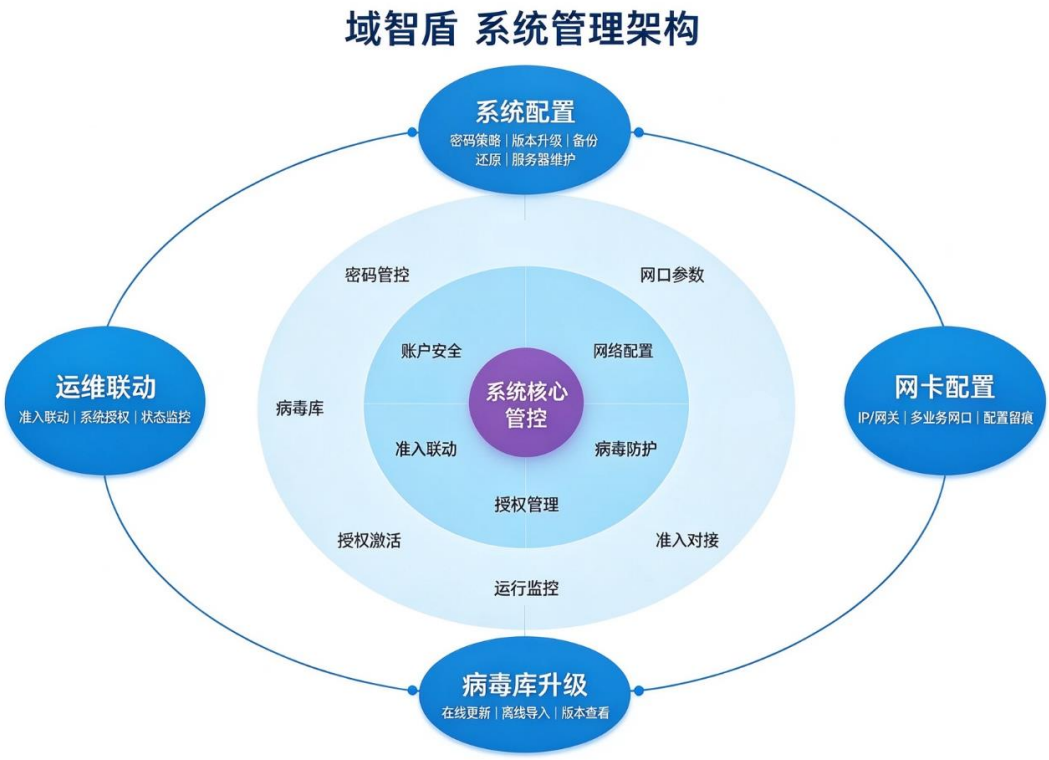


图 1-9 系统管理

五、用户操作手册

本章从使用者视角说明功能构成。

5.1 登录账户

跨网文件交换系统服务端上线后，使用者在所在网络内输入对应的内网或外网登录地址，进入登录界面，使用管理员分配的账号与密码登录。系统按账户所属网络区域自动进入相应空间，同一账户不可跨区域访问。

首次登录须修改初始密码；连续输错超过设定次数账户将被临时锁定；登录失败、异地登录与密码变更均记录在案。对于外部合作方，登录地址与有效期由管理员单独设定，到期后账户自动失效。

5.2 核心功能

5.2.1 我的上传

登录后进入上传文件列表，可查看本人上传文件的基本信息，包括文件名、文件大小、上传时间与当前状态。使用者可据此判断文件处于待审批、审批中、已放行还是已拒绝，无需另行询问，是使用者了解自身申请状态的重要入口。



图 1-10 我的上传

5.2.2 分享给我

他人分享给当前账户的文件集中呈现于该视图，显示文件名、文件大小、分享时间、有效时间、状态与分享者。有效期内的文件可预览、下载、再次分享与查看详情；已过期的文件保留记录但不可操作，避免使用者在不知情的情况下反复尝试。

该视图使“别人发给我的文件”与“我自己上传的文件”在系统内分离，减少混淆，也使分享关系可追溯——每份文件都能对应到具体分享者与分享时间。



图 1-11 分享给我

5.2.3 群文件

群文件按使用者所属的群组组织，呈现被分配到的群组内共享文件。群组通常对应项目组、专项工作组或部门，成员共同可见，避免同一份材料在成员之间反复单独传递。群组由管理员建立并维护成员，成员变动即时生效，离组人员不再可见。



图 1-12 群文件

5.2.4 我的分享

该视图呈现本人已分享出去的文件，显示文件大小、分享时间、有效时间与状态。使用者可对分享中的文件执行在线查看、下载与撤回；撤回后链接即时失效，避免文件在有效期外继续扩散。

对即将到期的分享，系统提示续期或重新分享，便于使用者在业务需要时主动处理，而不是等对方反馈“链接打不开”。

5.2.5 审批任务

被指定为审批人的使用者，在审批任务视图中处理待办。界面呈现申请名、申请人、申请原因、文件清单与检查结果，审批人据此作出批准或拒绝。拒绝须填写原因，原因回传申请人并在日志中留存。

审批人可查看附件详情与历史审批记录，对同一申请人的重复申请可参考历史判断，减少重复审阅。若审批人临时离岗，可通过委托审批将待办转交指定人员，委托关系与转交记录一

并留存。

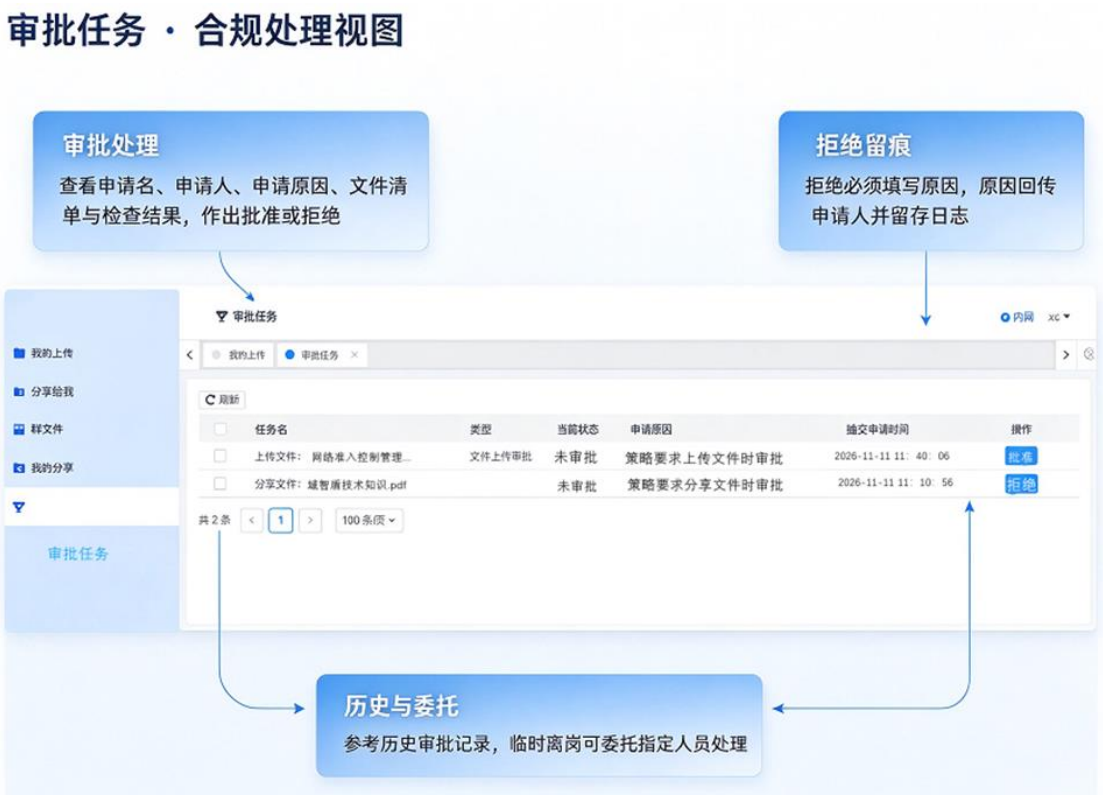


图 1-13 审批任务

六、代表企业

河北中视新研软件开发有限公司，从事终端安全、数据防泄漏与跨网数据交换方向的软件研发与交付。公司围绕“终端可管、数据可控、跨网可审”三条产品线开展研发，跨网文件交换系统是其中面向网络边界数据流转的产品。

研发与服务中心设于河北省石家庄市，具备从需求调研、方案设计、试点部署到上线运维的完整交付能力，公司为每个客户指定一名工程师负责售后，提供长期电话、QQ、Email 等多种方式的远程支持；客服热线 400-097-8770。

七、资质与荣誉

公司在产品认定、安全检测与信用评价方面取得的资质如下。



图 1-14 资质与荣誉

八、实践案例

以下案例来自实际项目，企业名称、区域数量、账户规模与时间节点已做脱敏处理，数据取自实施期与上线后前两个季度的运行记录。

公司简介

区级行政机关，下设十余个科室与若干事业单位，办公终端数百台，涉密网络与非涉密网络物理隔离。

日常需从非涉密侧导入政策文件与参考资料，向非涉密侧导出待审文稿；保密要求严格，检查频次高；人员计算机水平差异较大。

核心痛点

导入导出依靠保密专员一人操作，形成单点瓶颈，专员请假则业务停滞；

纸质审批单与文件不绑定，检查时无法证明“批准的就是这份文件”；

历史交换记录靠手工台账，追溯困难。

解决方案

划分涉密区与非涉密区两个网络区域；

设置三级审批模板，科室负责人、保密专员、分管领导依次审批，支持委托审批以解决单点问题；

涉敏审查配置敏感词库，命中后转人工复核；

申请记录与任务处理日志按月导出，作为保密自查材料。

应用价值

交换不再依赖单人，专员离岗期间流程仍可运转，月度自查材料由系统导出，准备时间从两天缩短到半小时，上线后未出现越权导出记录。

九、未来安全趋势展望

9.1 隔离会更严格，交换需求不会减少

等级保护与行业监管对网络边界的检查仍在细化，物理隔离与逻辑隔离的要求不会放松。与此同时，业务协同、外部交付、供应链协作带来的跨域数据流转只会增加。两者叠加的结果是：正式交换通道将从“可选项”变成“必选项”，且必须可审计。

9.2 交换系统将与数据分类分级打通

当前多数系统的检查依据是敏感词与文件类型，较为粗放。下一步的方向是与单位的数据分类分级结果对接：文件在进入系统时即带上密级与类别标签，审批层级、检查强度、有效期限随之自动匹配，减少人工判断带来的不一致。

9.3 检查能力将从“查病毒”扩展到“查内容”

病毒查杀已是基础能力。文本抽取、图片文字识别、结构化字段识别正在成为新的检查手段，用于判断文件中是否包含个人信息、客户清单、未公开的财务数据。检查结果不再是“通过或不通过”，而是给出风险类型与处置建议。

9.4 从单点系统走向跨域协同

企业之间的数据交付正在形成链式结构：主机厂与零部件商、医院与医联体、设计院与施工方。未来的交换能力需要支持跨组织的可信传递——发送方与接收方各有系统，通过标准接口对接，交付凭证双方互认，而不是一方发链接、另一方手工下载。

9.5 运营指标将被量化

跨网交换的管理将从“有没有系统”转向“系统用得好不好”，可量化的指标包括：正式通道使用率、平均放行时长、审批一次通过率、检查命中率、越权尝试次数。这些指标一旦成为考核项，系统价值才能被真正看见。

版权说明

版权所有：河北中视新研软件开发有限公司，保留全部权利。

文档中引用的部分专家、厂商观点，仅用于行业交流分享。未经本公司事先书面许可，任何单位、个人不得转载、复制、传播本资料内容。确因工作、学术研究需要引用本报告信息的，应当规范注明内容出处。

免责声明

本白皮书由河北中视新研软件开发有限公司编制，用于说明跨网文件交换系统的技术立场、能力框架与实施方法。

本文件所载内容仅供信息参考，不构成任何形式的要约、承诺或合同条款。产品的具体功能、性能指标、交付范围与服务内容，以双方签署的合同与技术协议为准。

文中引用的法律法规与标准，以发布时点的公开文本为准，相关法规与标准可能随政策调整而变化，读者应自行核实其现行有效性。本文件不构成法律意见。

本公司保留在不另行通知的情况下对本文件内容进行修订与更新的权利。最新版本以公司正式发布为准。

河北中视新研软件开发有限公司

域智盾软件　运营部

二〇二六年十一月

客服热线　400-097-8770

www.yzdsaas.com

地址　河北省石家庄市