证券代码：300659　　证券简称：中孚信息　　公告编号：2024-016

中孚信息股份有限公司

2023 年年度报告摘要

2024 年 3 月

一、重要提示

本年度报告摘要来自年度报告全文，为全面了解本公司的经营成果、财务状况及未来发展规划，投资者应当到证监会指定媒体仔细阅读年度报告全文。

所有董事均已出席了审议本报告的董事会会议。

大华会计师事务所(特殊普通合伙)对本年度公司财务报告的审计意见为：标准的无保留意见。

本报告期会计师事务所变更情况：公司本年度会计师事务所由变更为大华会计师事务所(特殊普通合伙)。

非标准审计意见提示

□适用 ☑不适用

公司上市时未盈利且目前未实现盈利

□适用 ☑不适用

董事会审议的报告期利润分配预案或公积金转增股本预案

□适用 ☑ 不适用

公司计划不派发现金红利，不送红股，不以公积金转增股本。

董事会决议通过的本报告期优先股利润分配预案

□适用 ☑ 不适用

二、公司基本情况

1、公司简介

股票简称	中孚信息	股票代码	300659
股票上市交易所	深圳证券交易所		
联系人和联系方式	董事会秘书	证券事务代表	
姓名	孙强	刘宁	
办公地址	济南市高新区经十路 7000 号汉峪金谷 A1-5 号楼 25 层	济南市高新区经十路 7000 号汉峪金谷 A1-5 号楼 25 层	
传真	0531-66590077	0531-66590077	
电话	0531-66590077	0531-66590077	
电子信箱	ir@zhongfu.net	ir@zhongfu.net	

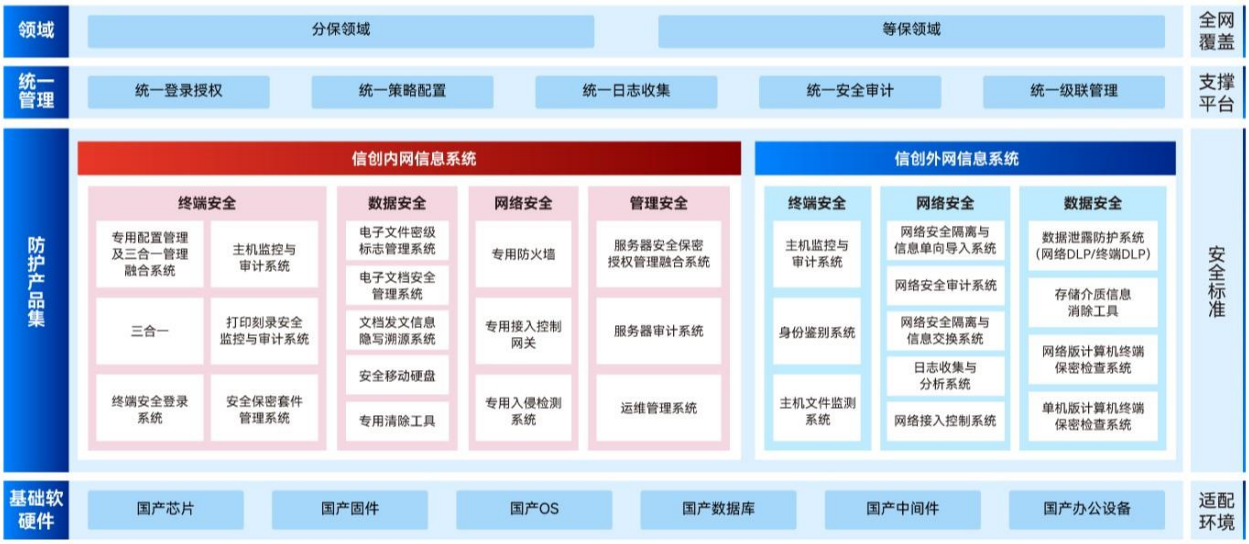
2、报告期主要业务或产品简介

报告期内，公司主营业务未发生重大变化，主要产品线及服务包括：主机与网络安全、数据安全、安全监管平台、检查检测、密码应用五条产品线及信息安全服务。同时，为满足用户安全需求、为用户持续创造价值，公司基于用户典型应用场景，围绕基于信创安全防护、安全监测预警、基于零信任的数据安全三大业务主线，打造面向党政、央国企、特殊行业用户的场景化解决方案，推动公司业务由产品销售向平台化、体系化解决方案营销模式演进，持续提升公司市场挖掘能力、业务布局能力，构建以产品及解决方案驱动公司业务发展和客户价值提升的良好局面。

1、主要产品体系

（1）主机与网络安全产品

公司主机与网络安全产品线适配主流国产 CPU、国产操作系统、国产数据库及国产中间件，围绕主机审计、终端安全登录、打印刻录审计、网络控制与传输等方面打造了完整的产品体系。



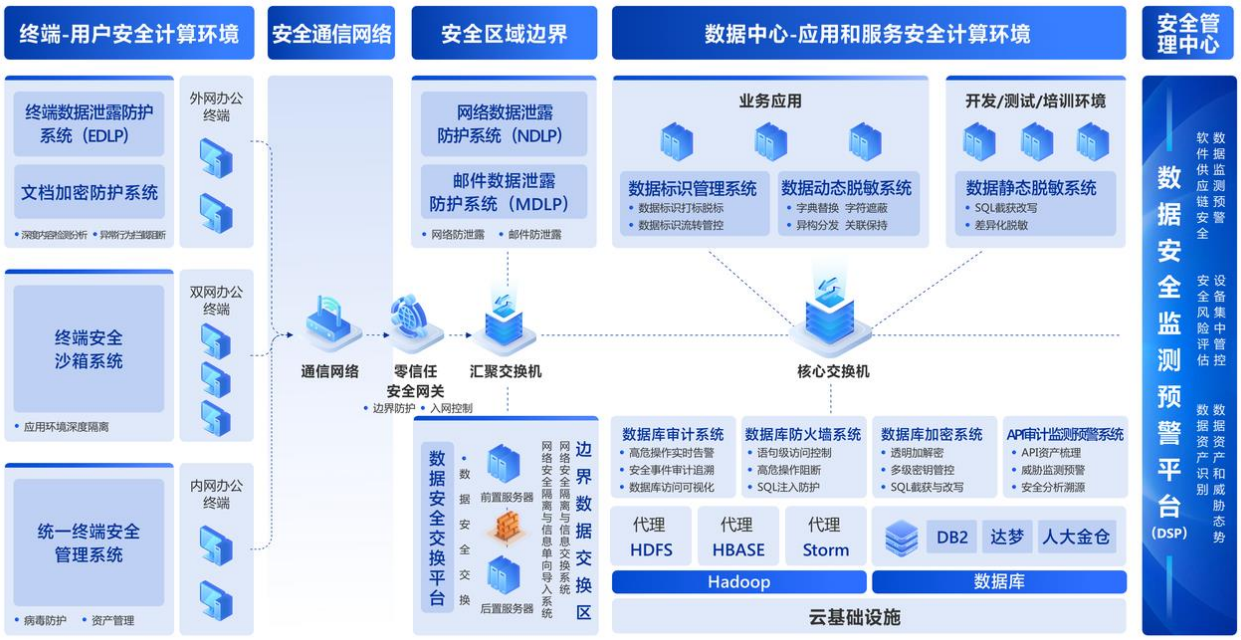
公司主机与网络安全主要产品简介：

主机与网络安全产品	
主要产品名称	**产品简介**
安全保密套件管理系统	系统通过整合终端安全技术和模块，对终端提供有效的、持续的安全防护。
计算机及移动存储介质保密管理系统（三合一）	具有阻断内网计算机违规外联、防止移动存储介质交叉使用、外部信息单向导入内网计算机三方面的功能，能够切实解决和防范内网计算机违规连接互联网和移动存储介质在内网计算机与外网计算机之间交叉使用引起的安全问题。
服务器安全授权管理系统	实现对信创服务器的安全授权和统一集中管理，对专用服务器从登录控制、专用存储介质管理、端口控制、磁盘控制等方面进行全面的保护和管理，满足管理员远程控制需求，有效提高专用服务器使用的安全性，降低设备维护的复杂度。
主机监控与审计系统	能够实时监控多种计算机操作行为，发现异常违规行为并产生报警，全面知悉和有效控制单位内部用户对主机资源和网络资源的使用，防止内部违规行为的发生。
终端安全登录系统	采用登录 KEY 和口令（PIN 码）双因子结合的身份认证技术，实现对登录用户身份授权与鉴别管理，从而有效防止用户非授权登录，保证终端系统及数据安全。
打印刻录安全监控与审计系统	实现用户与实体打印、刻录设备的隔离，并通过人员权限管理、设备授权管理对用户行为进行实时监控，进而完成文档输出全过程的监控和管理，并且形成了完备的审计日志，方便对文件输出情况进行统计和追溯，有效解决了文件输出过程中的审核和监管难题。
服务器审计系统	针对服务器系统的行为审计产品，可以实时监控多种服务器操作行为，实时发现异常违规行为并产生报警，为用户服务器安全提供保障。
网络运维管理系统	以平台化思路进行软件架构，对内部往来的通用软硬件设备状态进行实时监控，在发生故障或指标异常时进行告警。系统采用智能化思想，运用大数据技术，进一步提高 IT 运维效率，并与其他运维产品无缝结合，构建统一运维、统一监管、统一防护的有机体。
网络安全隔离与信息单向导入系统	设备关键硬件采用国产自主可控的元器件，系统利用光的单向传输特性构建了一条安全、单向的传输通道，实现了外网到内网的数据传输，保证敏感数据不泄露。
网络安全隔离与信息交换系统	采用自主研发的双通道隔离交换模块，实现在网络之间双向“摆渡”数据，解决了用户在不同网络之间双向数据交换的需求，同时利用病毒检查、内容安全检查、标志检查等策略保证数据在不同网络之间安全受控传输，使不同网络之间的业务可以高速、可靠、安全的进行数据交换。
数据安全交换平台	配合网络安全隔离与信息单向导入系统或者网闸设备，实现跨边界数据交换。该产品可极大拓展跨网数据交换能力，实现文件交换、数据库交换、接口服务交换、应用协议代理、音视频交换五大核心交换功能。解决多类型业务数据及海量数据共享交换难的问题，满足各领域客户对安全性、合规性、可靠性、高性能、兼容性和强审计的要求。
网络接入控制系统	以终端计算机和网络设备作为管理对象，对目标网络内终端进行合规审查、安全检查等，对不合规用户或者特定部门进行安全隔离保护。可保证合规用户的网络畅通，同时杜绝非法用户接入可能带来的安全隐患。
网络安全审计系统	通过分析网络中的通信流量，审计网络安全事件，生成安全统计报表，对重要安全事件或行为

	进行风险分析、追查取证，并为网络安全大数据分析系统提供有效的数据支撑。
入侵检测系统	系统能够实时高效发现网络中的异常流量，精准识别网络流量中的攻击行为，具备强大的攻击特征库，集成了海量的威胁情报库，实现对网络的实时监控，保护用户网络安全。
零信任 TNA 安全网关	不依赖 CPU、操作系统和第三方代码库的纯硬件高保障安全网关（Guarantee Advanced Trusted Network Access，TNA），基于零信任理念，以身份为基石，采用最小授权、持续信任评估、动态访问控制等机制，保障企业在互联网上的安全接入和业务访问安全。
统一终端安全管理系统	通过持续监控终端活动行为，检测安全风险，提供终端资质管理、网络准入、终端审计、安全管控、补丁管理、应用市场、统一策略管理等功能，对终端进行综合性安全防护。

（2）数据安全产品

公司数据安全产品以重要数据和敏感数据的防泄漏、防窃取、可追溯为目标，采用数据加密、数据保护、数据管控等技术，结合业务应用场景，实现对数据资产的可知、可控、可管，并且广泛兼容适配主流国产 CPU、国产操作系统、国产数据库及国产中间件。



数据安全主要产品简介：

数据安全产品	
主要产品名称	**产品简介**
电子文件密级标志管理系统	支持办公、PDF、音频、视频等各类进程和各种格式，满足多种工作场景需求。系统围绕电子文件的产生、存储、处理、交换、销毁等全生命周期过程，实现电子文件密级标志警示、强制访问控制和监管审计等安全目标。
文档加密防护系统	以透明加解密技术为核心，应用国密算法对电子文件进行加密防护，根据权限策略对用户及群组进行授权和权限管控，结合细粒度的文件审计功能，使数据防泄密工作做到防范于未然。
电子文档安全管理系统	通过与密级标志技术结合及统一策略，对电子文档的操作行为进行安全管理、访问控制和安全审计，达到事前可定义、事中可控制、事后可审计的安全目标，从而实现对电子文档数据资产的细粒度、全方位的安全保护。
文档发文信息隐写溯源系统	采用先进图形几何变换技术，可在流式、版式文档中嵌入肉眼难以识别的信息，但通过识别软件可以恢复取证，从而定位文档的分发途径，以实现信息泄露后可追可溯的安全管理目标。
终端/网络/邮件数据泄露防护系统（EDLP/NDLP/MDLP）	基于内容识别、敏感数据发现技术，监控终端用户文件操作行为，解析网络流量，提供事前预警、事中保护、事后追溯的技术手段，防止端、网、云等场景下的数据泄露和扩散。
终端安全沙箱系统	采用密码技术在移动终端/PC 终端打造安全可信的隔离环境，实现个人生活区及工作区的隔离。提供周密的安全认证机制、访问控制机制，防止非法用户、未授权用户进入受保护的工作

	区，保证业务系统中重要数据处理安全。
数据库防火墙	基于数据库协议分析与控制技术，实现数据库的访问行为控制、高危操作拦截、可疑行为审计，系统提供智能学习、内置规则、自定义规则等防护机制，实现对风险行为的拦截、主动预防和实时审计。
数据库加密系统	基于透明加解密技术实现敏感数据加密存储，通过细粒度访问控制、多级秘钥保护和秘钥周期轮换技术，实现数据库表级别和字段级别的精准防护，有效防止敏感数据泄露。
数据库审计系统	基于数据库协议解析技术，通过动态基线保护、访问与反馈双向审计、中间件关联审计、非法操作阻断等技术防止越权使用、权限滥用、权限盗用等安全威胁，满足各类法规对数据库审计的要求。
数据脱敏系统	基于数据去标识化技术，通过数据抑制、置空、随机、仿真和加密等多种脱敏方式满足生产环境、测试开发环境等场景敏感数据保护，同时促进数据开发和利用。
API 审计监测预警系统	以 API 资产为核心，通过对 API 资产的发现、检测、防护、响应，帮助组织梳理 API 资产，发现潜在的安全风险和异常行为，及时监测和应对 API 安全威胁，保护 API 资源的安全性，并提供实时预警和安全报告。
数据标识管理系统	系统提供文件的数据标识生成、脱标功能，通过基于面向切面的数据安全技术为应用系统提供透明的数据标识识别及流转管控能力，实现轻量化的数据安全访问控制和追踪溯源。
数据资产识别与安全风险评估系统	系统参照《网络数据安全风险评估实施指引》，根据国家、行业相关标准规范为用户提供数据资产梳理和分类分级服务，从安全管理、数据处理活动、数据安全技术、个人信息保护等方面对数据安全风险进行评估，指导数据安全防护建设。
软件供应链安全治理系统	系统具备软件成份分析、软件验收、上线检查、运行监管等功能，确保所用软件产品和服务不带有恶意代码、安全漏洞，不侵犯用户的隐私和危害数据安全。
数据安全监测预警平台	针对敏感、重要数据全生命周期进行安全风险监测，可接入数据库审计、数据加密、数据脱敏、数据防泄漏等防护组件，统一管理策略，掌握数据安全风险并快速响应处置，实现数据可见、可控、可管，构建体系化的数据安全防护能力，为业务的稳定、可靠运行提供保障。
数据安全态势感知系统	以数据安全全生命周期管理为核心，通过多维度量化指标，精准描述数据安全的实时风险及整体状况；利用海量数据分析引擎机及模型实现对数据风险的主动发现、精准定位、智能研判、快速处置、严格审计，完成对数据安全保护工作的闭环处置流程。

（3）安全监管平台

公司安全监管平台深度融合大数据、人工智能和数据可视化技术，有效整合内网、外网和互联网的各类数据，以提升党政机关和央国企用户网络安全态势感知、监测预警和应急处置能力为目的，通过对重要数据和敏感数据的深度挖掘、关联分析和追踪溯源，实现对客户网络安全风险的“全网络感知、全区域同控、全时段同管”能力，支撑重要用户网络防护和监管由基本防控向攻守兼备转型升级。

安全监管平台主要产品简介：

安全监管平台	
主要产品名称	**产品简介**
互联网接入口监测平台	由互联网接入口检测器、互联网接入口监测平台等部分组成，用于检测、分析、处置网络攻击窃密及传输敏感信息行为。
政务应用安全监测系统	系统依托政务服务平台，汇聚多种政务应用数据，精准锁定及管控敏感信息在政务应用中的发布、存储、处理、传输等行为，实现政务应用数据可接入、可分析、可监测，消除政务平台泄露敏感信息风险隐患。
互联网站内容监控系统	系统基于前沿搜索引擎、自然语言处理、智能分析等技术进行设计开发，帮助各级网络安全行政管理部门对辖区门户网站进行有效的安全检查与监控，及时发现泄密隐患，控制敏感信息在互联网门户网站的传播。
威胁情报平台	系统专注于高精准情报，为客户提供高性能、高可用、可扩展的威胁情报查询分析能力和威胁情报共享能力。
木马脱离调度系统	系统对含有恶意程序的有害文件进行去木马操作，将有害文件隔离，确保恶意程序不扩散。
追影攻击分析系统	统融合大数据、海量高质量威胁情报和专家知识库，有效检出 APT 攻击、窃密木马等高危恶意攻击行为，做到“让安全可看见”。
互联网失泄密智能分析平台	系统运用大数据分析、人工智能和数据可视化等技术，有效整合各类监管系统的数据，实现对互联网安全态势的全面监管、融合展示、动态管理、资源共享、协同联动、快速响应，全面提升网络监管能力。
网络安全管理与运行监管平台	为用户提供资产在线动态监管、基于分保的动态持续合规监管、违规行为及未知风险发现三种核心能力，构建安全运行监管能力、违规行为发现能力、攻击行为发现能力和全网应急处置等核心能力，打造可视化的安全监管态势感知。
重要场所电磁环境长时监测系统	该系统能够解决重要场所中违规信号和异常无线发射信号的检测难题，通过实时采集场所内存在的无线信号，实现异常电磁信号的告警，同时结合信号分析功能和后端信号特征库自动匹配功能，可实现对异常发射信号频点、带宽、调制方式及内容的识别和还原，为重要单位的电磁空间安全提供保障。
保密综合态势感知平台	系统运用深度融合监测和检查相关数据，打通数据壁垒、全面深化数据分析、提升智能辅助决策和协同作战能力。打造安全监测预警、应急响应和追踪溯源于一体的综合态势感知平台。

（4）检查检测产品

公司检查检测产品围绕主机安全、数据库安全、邮件安全、移动终端安全、云存储安全，通过构建网络化部署、自动化检查、实时化检测、便捷化整改、智能化分析于一体的检查检测系统，实现实时发现违规行为，有效提高安全能力。

检查检测主要产品简介：

检查检测产品	
主要产品名称	**产品简介**
计算机终端保密检查系统	包括单机版和网络版，通过主机检查、终端自查、违规判定等，及时发现违规行为、失泄密隐患和安全漏洞，做到有效防止失泄密事件发生，保障国家秘密的安全。
数据库内容保密检查系统	系统主要针对各类型数据库弱口令、数据库安全策略配置、数据库敏感内容进行详细检查，及时发现违规存储行为和安全隐患，确保重要数据和敏感数据安全，支持对云存储、云数据库及主流国产数据库的检查。
电子邮件内容保密检查系统	系统实现对个人邮箱、个人邮件客户端及单位邮件服务器中存储的电子邮件的邮件头、正文、附件敏感性检查，及时发现违规传递行为和安全隐患，确保敏感信息数据安全。
移动终端保密检查系统	系统集成高效反病毒引擎及丰富病毒库，同时针对移动终端文件、图片、应用等进行检查，及时发现敏感信息、木马病毒应用，实现对移动终端的全面化、高效化检查。
云存储内容保密检查系统	系统通过适配各云存储官方 SDK，利用数据抽取、数据分析等技术，结合完整的数据与合规策略模型，实现对单位公有云及私有云存储中存储的文档、图片、压缩包等数据进行自动化敏感内容检查，及时发现违规存储行为和安全隐患，确保敏感信息数据安全。
敏感信息实时监管系统	将定期、不定期安全检查转变为实时监控，及时发现泄密隐患并堵住泄密漏洞。系统对所监控终端中所有文档的操作行为进行监控，留存操作日志供事后溯源查证，同时根据策略自动分析文档的敏感程度，发现异常后可屏蔽计算机网络功能，并向管理部门报警，防止泄密行为发生。
网络测评管理系统	依据分级保护测评标准，面向全国测评机构，辅助进行网络保护测评、风险评估、应用系统评估，实现测评全流程信息化管理，并针对现场检测环节提供专用现场检测系统及测评工具集，有效提升测评工作效率与能力。

（5）密码应用产品

公司以国产密码算法和行业标准为基础，开发了从客户端、服务端到系统类一系列密码产品。

密码应用主要产品简介：

密码应用产品	
主要产品名称	**产品简介**
密码服务管理平台	密码服务管理平台是一套具备密码服务按需配置、密钥集中管理、统一提供服务接口、统一设备管理能力以及密码安全态势感知能力的密码服务、管理、监控一体化平台。能够提供合规的一站式密码改造方案，兼容多种密码硬件，屏蔽底层复杂逻辑，简化应用系统改造难度，支撑密码测评改造快速落地。按需提供弹性可扩展的云密码资源池，提高设备利用率，满足未来动态扩展性需求。
服务器密码机	中孚 HSS 服务器密码机是自主研发的密码安全模块，适用于高速运算的密码安全应用场合，满足应用系统数据的签名、验证、加密、解密要求。保证传输信息的机密性、完整性、有效性。可作为数字证书管理、密钥管理、身份管理、接入认证、数据安全交换、数据存储加密、数字内容保护等系统的基础核心密码设备，支持 SM2/SM3/SM4 等国产密码算法和 RSA2048 等通用安全密码算法，可广泛应用于金融、政务、能源、工业控制、基础通信等行业。
云服务器密码机	云服务器密码机为适应云应用场景的密码资源服务平台，采用虚拟化技术，将整机系统划分成多个相互独立的虚拟密码管理运算单元，可以同时为云环境下多个租户的应用系统提供密码资源、运算资源、存储资源和基础安全支撑，满足用户对密钥安全管理和高效密码计算的需求，包括数字证书管理、密钥管理、身份管理、接入认证、数据安全交换、数据存储加密、数字内容保护、身份认证、电子签名、数据加密等。
密码卡	密码卡是包含支持 PCIe 接口和 SATA 接口的两款密码模块，具有高效密码运算能力和密钥安全管理能力，作为服务端密码应用系统核心组件，用于身份认证、通信加密、签名验证等各类应用场景。PCIe 接口密码模块的主机接口符合 PCIe2.0 工业标准，可以广泛兼容各种类型的机架式服务器和桌面服务器，SATA 接口密码设备具备符合 SATARevision3.0 标准（SATA6Gbps）的 SATADevice 接口，可以广泛应用在具备 SATAHost 接口的主机或服务器中。
智能密码钥匙	基于自主产权的操作系统开发的多功能终端密码产品，可以实现数字证书的生产存储、数字签名认证。
双界面智能 IC 卡	主要应用于电子营业执照载体，采用国产智能 IC 卡专用芯片，内嵌自主 COS 系统，实现输入输出管理、加密运算管理、命令解析管理和文件管理功能，同时具备密钥存储和密码运算能力，支持国密算法。

2、主要解决方案

围绕国家网络安全战略，公司聚焦数据安全，按照分级保护、等级保护、关基保护等法律法规，依据网信、公安、保密、密码等监管部门的相关要求，面向党政、央国企和特殊行业，构建了基于用户场景化的解决方案体系。

党政安全解决方案	
解决方案	**方案简介**

信创安全防护解决方案	中孚基于多年分保技术积累和测评经验，在统一基础平台上，打造了包含终端、网络、应用和数据防护为一体的安全解决方案，可实现信创平台与原有平台混合部署，实现统一管理、统一运维、统一审计，满足用户合规安全要求。
网络安全管理与运行维护解决方案	为便于机关单位实现内网资产可视化、防护实战化、分析智能化、运维规范化、体系化，本方案提供整网安全能力的统一管理、统一调度、统一处置，为用户带来所见即所得的安全价值。
商用密码应用安全性解决方案	为帮助用户通过密码测评，依据商用密码应用安全性相关法律法规，为用户提供商用密码应用咨询、国密改造、系统集成和密码测评服务，确保用户系统满足商用密码测评合规性、有效性要求。
跨网数据安全交换解决方案	为解决在内网和外网、不同涉密域之间数据便捷、高效、稳定和安全交换的问题，基于网络安全隔离交换技术打造的跨网数据安全交换解决方案，能够提供单向、双向等多应用场景数据安全交换、敏感数据内容分析、木马检测、传输控制等能力。
安全检查整改一体化解决方案	基于智能化内容分析引擎开发的安全检查整改一体化解决方案，主要为解决机关单位安全自查手段缺乏、工作繁重、整改不彻底等问题，实现泄密事件的事前预警、事中发现和事后溯源，满足机关单位日常安全自查和检查工作需求。
安全监测预警解决方案	围绕安全主管部门的监管需要，基于“统一防护、统一监管、统一运维、统一处置”理念设计的安全监管整体解决方案，能够实现对互联网、内网和电磁空间的全域全维检查监管，为用户提供便捷、易用的综合性智能分析处置平台，有效提升检查预警能力，实现“一屏观天下、一网控全局”的目标。
测评管理和风险评估解决方案	为实现测评工作规范化，减轻测评工作量，提升现场测评能力，打造的测评管理和风险评估解决方案，能够为测评部门提供测评任务流程化管理、现场测评数据自动化采集、测评报告智能化生成，可有效提升测评工作效率。机关单位版可为机关单位提供预测评、风险自评估能力。
电子文件全生命周期安全解决方案	以电子文档的安全易用为核心，站在用户的文件起草、文件定密、文件流转、文件使用、文件输出、文件溯源业务场景，基于文件标识技术，围绕电子文件全生命周期安全管理，利用丰富的多样化接口与应用系统无缝对接，融合密点识别、安全防护、检查监测、文件管控全系列安全产品和生态系统，实现电子文档资产清晰、集中存储、轨迹可溯、生态支撑的目标。
电磁空间检测解决方案	实现重要场所、公务车辆、临时会场等多业务场景下的电磁空间异常无线信号的发现识别，快速识别各类环境下的窃听、窃照、GPS 跟踪设备，并实现对异常信号的快速定位功能。
工作秘密信息防护解决方案	依据《工作秘密信息防护指南（试行）》要求，打造覆盖端管边云脑的工作秘密安全技术防护体系，强化终端信息防护、数据传输防护、应用系统防护、数据隔离交换、数据存储与备份及安全监测 6 项防护技术，确保机关、单位工作秘密处理活动的合规开展，逐步实现对工作秘密的细粒度管控。
央国企安全解决方案	
解决方案	**方案简介**
基于零信任的数据安全解决方案	针对全数据资产（结构化数据和非结构化数据）安全防护，融合沙箱技术与零信任理念，以密码为基石，关键业务安全为核心，全数据安全为目标，风险管理为导向，内容、行为分析为抓手，分析识别窃密、泄密、勒索三类主要安全风险，依托安全大脑，打造云、管、端、边全面防御架构，保障数据流转过程中处理、存储、传输、共享交换、服务运维等五类场景安全。
敏感信息泄漏风险预警解决方案	面向中央企业，基于多种敏感信息分析模型，通过一站式的检查方式，实现对计算机终端、数据库、云存储、移动端、电子邮件检查的全覆盖，实现检查工作态势分析，及时发现敏感数据，杜绝泄密隐患，为主管部门安全监督检查工作提供决策依据。
电网行业数据安全态势感知解决方案	数据安全防护和态势感知以数据资产动态管理、智能高效风险监控、数据安全事件响应与溯源、全生存周期策略管理为核心，以可视化为特色，以可靠服务为保障，逐步达到数据资产看得见、说得清、管的住、强审计、深溯源的目标。
中央企业商业秘密安全保护解决方案	面向中央企业，以商业秘密数据全生命周期管控为核心，全面支撑商业秘密管理、监督、检查、技术防护及培训教育等工作，提升中央企业商业秘密安全防护能力。
央国企安全管理业务数字化解决方案	覆盖央企集团的互联网、内网，在合规的基础上，帮助用户央企用户实现安全管理工作体系化、数字化、便捷化的目标，切实提升集团安全风险预警和应急处置的能力，推动集团单位安全管理工作转型升级。
终端跨域安全办公解决方案	在互联网和工作网逻辑隔离要求前提下，解决办公终端安全访问互联网问题，提升工作人员上网办公与数据共享操作体验，防范工作秘密敏感数据泄露

数据安全治理解决方案	通过对动静态数据资产存储、流转信息的采集分析、权益声明、分类分级，实现对数据资产底账的动态管理，识别重要资产、僵尸资产、幽灵资产、数据流向、数据热度等，为数据所有者提供数据资产权益保护支持。
特殊行业安全解决方案	
解决方案	**方案简介**
特殊行业综合安全防护解决方案	针对新时期特殊行业网络安全面临的新形势、新挑战，基于国产计算机软硬件平台，针对各级单位重要计算机、移动存储载体、重要文件等管理对象的新一代安全管理系统。
特殊行业网络安全监管解决方案	针对特殊行业互联网敏感信息的监测、预警、防护和应急处置的综合需求，打造全网重要信息抓取、数据高效解析、违规事件快速处置等能力，构建网络安全监测预警体系，实现“一屏观态势、一网控全局”。
安全服务解决方案	
针对当前行业发展趋势与客户安全需求的演变，构建“安全运营、安全咨询、应急响应、安全测试”梯次递进的安全服务体系，打造面向攻防实战、以对抗能力为核心的服务体系，为重要客户、重要信息系统提供系列安全服务、并持续提升服务质量与价值，为客户网络提供全方位的安全保障。	
安全教育解决方案	
为客户提供线上安全可靠、内容详实的安全与保密宣教平台，提供多种形式的前台学习资源，包括手机 App、微信小程序、PC 网页等，后台管理提供资源管理、考试问卷、综合分析等。依据不同建设需求可以私有化部署和 SAAS 化服务。中孚提供平台及资源、内容的运营服务，配合线上线下活动的运维支撑。	

3、主要会计数据和财务指标

（1） 近三年主要会计数据和财务指标

公司是否需追溯调整或重述以前年度会计数据
☑是 □否
追溯调整或重述原因
会计政策变更

单位：元

	2023 年末	2022 年末		本年末比上年末增减	2021 年末	
		调整前	调整后	调整后	调整前	调整后
总资产	1,689,528,982.00	1,863,499,136.10	1,873,352,991.34	-9.81%	2,175,260,897.08	2,186,938,712.23
归属于上市公司股东的净资产	982,567,397.33	1,185,583,586.40	1,185,583,586.40	-17.12%	1,675,645,392.29	1,675,645,392.29
	2023 年	2022 年		本年比上年增减	2021 年	
		调整前	调整后	调整后	调整前	调整后
营业收入	918,584,003.86	644,205,476.86	644,205,476.86	42.59%	1,270,043,341.90	1,270,043,341.90
归属于上市公司股东的净利润	-186,298,752.61	-446,914,514.62	-446,914,514.62	58.31%	116,872,921.19	116,872,921.19
归属于上市公司股东的扣除非经常性损益的净利润	-217,220,513.00	-468,418,102.88	-468,418,102.88	53.63%	95,885,851.76	95,885,851.76
经营活动产生的现金流量净额	-20,401,599.24	-345,871,124.43	-345,871,124.43	94.10%	100,105,312.82	100,105,312.82
基本每股收	-0.83	-1.99	-1.99	58.29%	0.52	0.52

益（元/股）						
稀释每股收益（元/股）	-0.83	-1.99	-1.99	58.29%	0.51	0.51
加权平均净资产收益率	-17.19%	-31.32%	-31.32%	45.11%	7.29%	7.29%

会计政策变更的原因及会计差错更正的情况

本公司自 2023 年 1 月 1 日起执行财政部 2022 年发布的《企业会计准则解释第 16 号》“关于单项交易产生的资产和负债相关的递延所得税不适用初始确认豁免的会计处理”。

（2） 分季度主要会计数据

单位：元

	第一季度	第二季度	第三季度	第四季度
营业收入	137,350,422.34	192,120,804.09	144,924,652.73	444,188,124.70
归属于上市公司股东的净利润	-115,307,192.95	-66,117,120.47	-84,736,834.00	79,862,394.81
归属于上市公司股东的扣除非经常性损益的净利润	-119,209,220.52	-67,425,317.18	-85,174,260.39	54,588,285.09
经营活动产生的现金流量净额	-153,433,173.85	-28,619,971.83	-53,009,974.76	214,661,521.20

上述财务指标或其加总数是否与公司已披露季度报告、半年度报告相关财务指标存在重大差异

□是 ☑否

4、股本及股东情况

（1） 普通股股东和表决权恢复的优先股股东数量及前 10 名股东持股情况表

单位：股

报告期末普通股股东总数	25,067	年度报告披露日前一个月末普通股股东总数	24,121	报告期末表决权恢复的优先股股东总数	0	年度报告披露日前一个月末表决权恢复的优先股股东总数	0	持有特别表决权股份的股东总数（如有）	0

前 10 名股东持股情况（不含通过转融通出借股份）

股东名称	股东性质	持股比例	持股数量	持有有限售条件的股份数量	质押、标记或冻结情况	
					股份状态	数量
魏东晓	境内自然人	25.38%	57,253,101.00	42,939,826.00	不适用	0.00
陈志江	境内自然人	14.02%	31,619,428.00	23,714,571.00	不适用	0.00
厦门中孚普益投资合伙企业（有限合伙）	境内非国有法人	3.04%	6,845,626.00	0.00	不适用	0.00
中孚信息股份有限公司－2022 年员工持股计划	其他	1.82%	4,103,200.00	0.00	不适用	0.00
孙强	境内自然人	1.81%	4,071,408.00	3,053,556.00	不适用	0.00
交通银行股份有限公司－汇丰晋信核心成长混合型证券投资基金	其他	1.22%	2,754,371.00	0.00	不适用	0.00

招商银行股份有限公司－汇丰晋信研究精选混合型证券投资基金	其他	1.21%	2,721,640.00	0.00	不适用	0.00
万海山	境内自然人	0.91%	2,047,654.00	0.00	不适用	0.00
魏冬青	境内自然人	0.48%	1,080,000.00	0.00	不适用	0.00
中国建设银行股份有限公司－汇丰晋信价值先锋股票型证券投资基金	其他	0.45%	1,026,100.00	0.00	不适用	0.00
上述股东关联关系或一致行动的说明	公司股东魏冬青系公司股东魏东晓之一致行动人。					

前十名股东参与转融通业务出借股份情况

□适用 ☑不适用

前十名股东较上期发生变化

□适用 ☑不适用

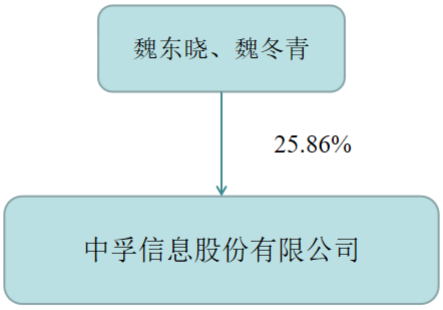
公司是否具有表决权差异安排

□适用 ☑不适用

（2） 公司优先股股东总数及前 10 名优先股股东持股情况表

公司报告期无优先股股东持股情况。

（3） 以方框图形式披露公司与实际控制人之间的产权及控制关系



5、在年度报告批准报出日存续的债券情况

□适用 ☑不适用

三、重要事项

公司于 2023 年 2 月 24 日召开第五届董事会第二十八次会议、第五届监事会第二十六次会议审议通过了《关于公司 2023 年度向特定对象发行 A 股股票方案的议案》等议案，并于 2023 年 3 月 13 日召开 2023 年第二次临时股东大会审议通过。公司于 2023 年 5 月 30 日召开第六届董事会第三次会议、第六届监事会第三次会议审议通过了《关于调减公司向特定对象发行股票募集资金总额暨调整发行方案的议案》等议案。2023 年 7 月 12 日，公司收到深圳证券交易所出具的《关于中孚信息股份有限公司申请向特定对象发行股票的审核中心意见告知函》，认为公司符合发行条件、上市条件和信息披露要求。2023 年 8 月 25 日，公司收到中国证券监督管理委员会出具的《关于同意中孚信息股份有限公司向特定

对象发行股票注册的批复》同意公司向特定对象发行股票的注册申请。公司向特定对象发行股票 34,851,621 股，每股面值 1.00 元，每股发行价格为 14.49 元，募集资金总额 504,999,988.29 元，扣除发行费用后实际募集资金净额 491,430,128.32 元。上述募集资金到账情况已经大华会计师事务所（特殊普通合伙）审验，并出具了《向特定对象发行人民币普通股（A 股）验资报告》（大华验字[2024]000017 号）。

中孚信息股份有限公司董事会

董事长：魏东晓

二〇二四年三月二十九日