

中国移动通信集团吉林有限公司信息技 术部经营分 析系统定级报告



2025 年 5 月 13 日

文档名称	中国移动通信集团吉林有限公司信息技术部经营分析系统定级报告
作 者	常剑飞
类 别	
子类别	

文件名称	中国移动通信集团吉林有限公司信息技术部经营分析系统定级报告			
摘 要				
修订历史(REVISIONHISTORY)				
版本号	日期	作者	审阅人	摘要
1.0	2008/1/31	徐党生		
1.1	2013/6/12	徐党生	王海燕	
1.2	2014/8/13	臧郝真	廉维	
1.3	2015/8/13	臧郝真	廉维	
1.4	2017/7/11	徐党生	廉维	
1.5	2018/9/6	常剑飞	廉维	
1.6	2019/7/11	常剑飞	王迪男	
1.7	2020/2/21	常剑飞	王迪男	
1.8	2022/10/15	常剑飞	王迪男	
1.9	2023/7/15	常剑飞	王迪男	
1.10	2025/5/12	常剑飞	王迪男	

目录

1	中国移动通信集团吉林有限公司信息技术部经营分析系统基本情况	5
1.1	系统概述	5
1.1.1	业务/应用范围	5
1.1.2	服务范围	6
1.1.3	用户类型	6
1.2	管理情况	6
1.2.1	所属单位基本情况	6
1.2.2	安全管理架构	6
1.3	技术情况	7
1.3.1	物理环境	7
1.3.2	网络拓扑结	8
1.3.3	硬件设备部署情况	8
1.3.4	网络边界	12
2	中国移动通信集团吉林有限公司信息技术部经营分析系统安全等级的确定	12
2.1	安全等级定级计算方法	12
2.1.1	社会影响力	13
2.1.2	规模和服务范围赋值	14
2.1.3	提供服务的重要性赋值	14
2.2	中国移动通信集团吉林有限公司信息技术部经营分析系统安全保护等级	15

1 中国移动通信集团吉林有限公司信息技术部经营分析系统基本情况

1.1 系统概述

中国移动通信集团吉林有限公司信息技术部经营分析系统，基于分布式数据库、分布式文件系统等大数据云计算技术，建设“应用层”与“数据层”深度解耦的经营分析系统，具备八层功能架构：数据源层、数据采集层、数据存储层、数据计算层、数据服务层、数据管控层、平台层、应用层，在数据管控驱动下的新型经营分析系统，实现对中国移动通信集团吉林有限公司信息技术部B域、O域、M域等各类数据的集中存储、关联分析、数据服务能力。

1.1.1 业务/应用范围

中国移动通信集团吉林有限公司信息技术部经营分析系统业务范围包括KPI指标监控、统计报表、综合分析和数据挖掘。

KPI指标监控功能是借助表格和图形方式，对公司KPI指标的完成情况进行实时的监控，使分析人员和各级管理者能够及时了解目前各项指标的完成进度，并对不同指标之间、不同分公司之间的完成进度进行比较分析。

统计报表功能是根据预先设定好的项目、数据、格式等需求，按照一定的周期定期，生成统计结果数据，进行汇总或分析处理，形成规定格式的报表。报表生成具有很高的灵活性，支持按指定时间段自动汇总、统计各级报表数据自动生成汇总报表，支持选择各种统计元素。同时，报表模板设计、开发难度小，方便操作。目前，报表是经营分析系统最主要的功能。

综合分析是基于OLAP的多维分析技术。按照轴、面、群的分析方法，对指标从品牌、客户变化、ARPU、时间、地区、用户特性等维度进行层层分解，并对分解出的群中包含的内容进行综合分析，分析内容可以包括客户数、收入、业务量分析、新业务等。综合分析根据某个分析主题，选择与主题相关的分析内容，对指标进行层层分解

高级数据挖掘是利用数据挖掘方法和技术，从大量的数据中寻找数据之间的关系模式。高级数据挖掘内容包括客户价值分析、业务预测、消费层次变动分析、客户流失分析、客户细分等。这类分析涉及的变量数目多，变量的关系复杂，数据分布缺少较强的规律性，因此分析的综合性、难度和深度较大，对分析人员要求很高。

1.1.2 服务范围

中国移动集团吉林有限公司、中国移动通信集团吉林有限公司信息技术部。

1.1.3 用户类型

中国移动信息技术部内部人员。

1.2 管理情况

1.2.1 所属单位基本情况

中国移动信息技术部为有效支撑中国移动“大连接”战略,落实 IT 领域改革部署,建立“架构先进、运营高效、内外兼顾”的大 IT 体系,中国移动整合原集团公司业务支撑系统部、中国移动(深圳)有限公司和南方基地 IT 支撑团队,成立中国移动信息技术部。中国移动信息技术部的成立,是中国移动 IT 能力提升的重要标志,也是中国移动打造 IT 核心竞争力的新起点。

中国移动信息技术部对集团内部承担集中化 IT 系统的运营和支撑,重点推进 IT 统一规划、企业级大数据平台、集中化 IT 系统的整合与建设等各项工作,为内部各单位提供资源共享、能力集中、合理管控的 IT 运营支撑服务,协助各单位打造极致体验、高效运营、良性增长的数字化服务能力。对外部客户,依托集中化 IT 系统和自主研发经验积累,积极探索 IT 资源和能力优势的对外输出,面向其他行业企业和海外电信运营商提供大数据等 IT 解决方案和服务,努力拓展对外服务收入份额,力争成为业界有影响力的专业化 IT 服务机构。

1.2.2 安全管理架构

中国移动信息技术部建立了由决策层、管理层和执行层构成的完整统一的安全组织架构。在总公司设立网络安全领导小组,领导小组是中国移动信息技术部网络安全管理的最高决策机构;中国移动信息技术部网络安全领导小组组长由公司党委书记、总经理担任,副组长由公司党委委员、副总经理担任;中国移动信息技术部党委对网络安全工作负有主体责任,党委书记是第一负责人。网络安全领导小组办公室设在安全管理中心;在各部门、生产中心内设置信息安全

管理岗，负责执行各自部门的信息安全管理工作。

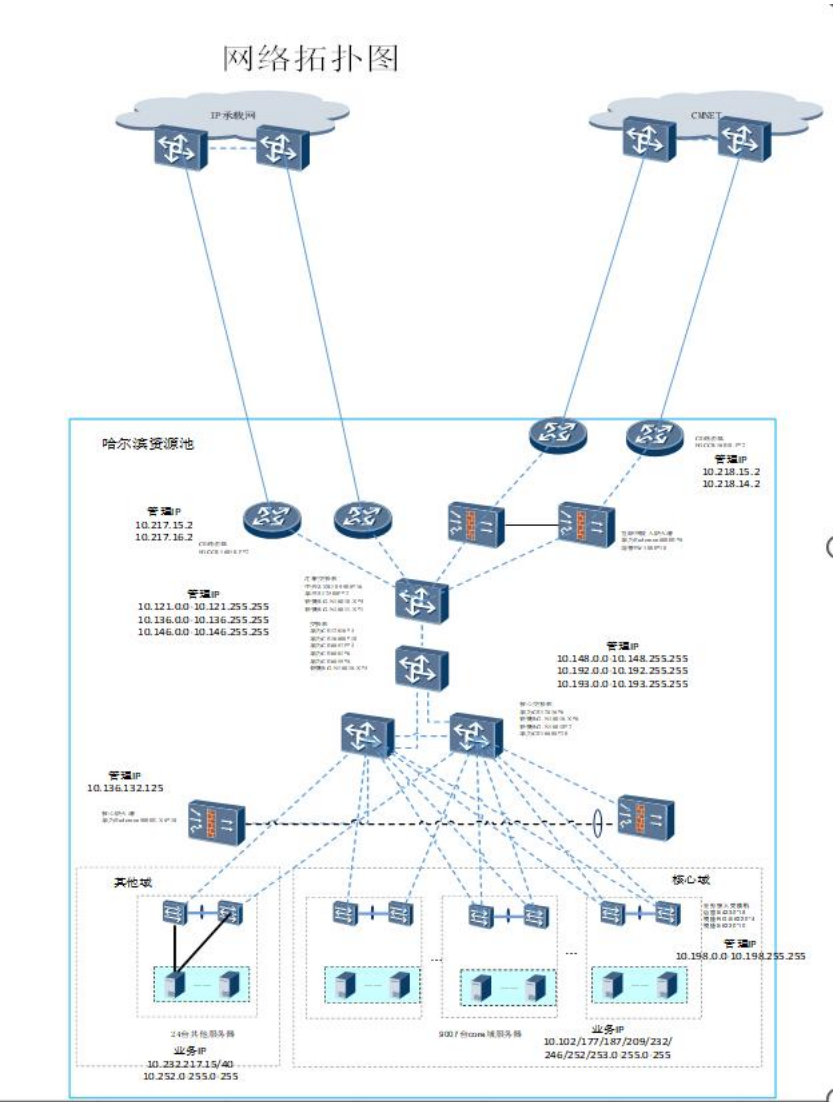
根据“谁主管谁负责、谁运营谁负责”的管理原则，在公司整体安全保障体系下，信息安全小组负责信息网络的日常安全管理，同时进行安全防护系统的开发建设和管理维护工作。

1.3 技术情况

1.3.1 物理环境

经营分析系统主机、设备主要放置在黑龙江省哈尔滨市平房区哈南 17 路 13 号 哈池-B14-POD15(BM)，机房建设和管理均严格按照国家规范及相关要求，安装了火灾自动报警系统、气体灭火系统、空气抽样早期报警系统，确保要害部位的消防安全；在机楼(房)的外部安装有闭路电视监控系统，由保安值班室以及监控人员实行 24 小时监控，保障要害部位内外治安环境的安全；由专职人员每日对构建基础网络环境以及系统运行环境的 UPS、蓄电池机房进行电压、电流例行检查，发现异常情况立刻报障处理，严格按照故障处理流程处理相关安全事件；人员进出机房会在机房进出登记表中进行登记，并在机房门禁系统留下日志记录，安全管理员对机房门禁日志以及机房进出记录定期进行审阅，检查是否有异常进出情况。

1.3.2 网络拓扑结



1.3.3 硬件设备部署情况

中国移动通信集团吉林有限公司信息技术部经营分析系统设备主要在黑龙江省哈尔滨市平房区哈南 17 路 13 号 哈池-B14-POD15(BM) 机房，具体部署情况如下：

类型	品牌	型号	IP	IP 数量	所在机房
----	----	----	----	-------	------

服务器	中兴	R5300 G4	10.102.42.195 10.102.42.194 10.102.42.18 10.102.42.30 10.102.42.69 10.102.42.169 10.102.42.59 10.102.42.117 10.102.42.22 10.102.42.166	10	黑龙江省哈尔滨市平房区哈南 17 路 13 号 哈池-B14-POD15 (BM)
服务器	中兴	R8500 G4	10.252.92.143 10.252.92.151	2	黑龙江省哈尔滨市平房区哈南 17 路 13 号 哈池-B02-POD8 (BM)
服务器	超聚变	2488H V5	10.252.92.103 10.252.92.108	2	黑龙江省哈尔滨市平房区哈南 17 路 13 号 哈池-B02-POD8 (BM)
交换机	华为	NE40E	192.168.108.1 192.168.108.2	2	哈尔滨资源池 B02-PUB
交换机	中兴	ZXR10 9916	10.193.98.1 10.193.98.1 10.193.98.2 10.193.98.13 10.193.98.3 10.193.98.14 10.193.98.4 10.193.98.15	8	哈尔滨资源池 B02-PUB
交换机	锐捷	N18018	10.198.1.1 10.198.1.1 10.198.1.5 10.198.1.6 10.198.1.7 10.198.1.8	6	哈尔滨资源池 B02-POD8

交换机	锐捷	S6220	10.198.12.41 10.198.12.42	2	哈尔滨资源池 B02-POD8
交换机	华为	CE16808	10.136.171.1 10.136.171.2 10.136.171.3 10.136.171.4 10.136.171.5 10.136.171.6	6	哈尔滨资源池 B14-POD15
交换机	华为	CE6857F	10.148.47.41 10.148.47.42	2	哈尔滨资源池 B14-POD15
交换机	锐捷	RG-N18018-X	0.136.148.12 10.136.149.12 10.136.148.13 10.136.149.13 10.136.148.14 10.136.149.14 10.136.148.1 10.136.149.1	8	哈尔滨资源池 B14-PUB
路由器	华为	NE40E	192.168.108.3 192.168.108.4	2	哈尔滨资源池 B02-PUB
路由器	华三	CR16018-FA	10.136.148.2 10.136.149.2	2	哈尔滨资源池 B14-PUB
防火墙	华三	M9010	10.193.98.5 10.193.98.5 10.193.98.6 10.193.98.6	4	哈尔滨资源池 B02-PUB
防火墙	迪普	FW1000	10.198.1.13 10.198.1.13	2	哈尔滨资源池 B02-POD8
防火墙	华为	Eudemon9000E-X8	10.136.171.13 10.136.171.14	2	哈尔滨资源池 B14-POD15

防火墙	华三	M9016-V	10.136.148.3 10.136.148.3	2	哈尔滨资源池 B02-POD8
主机防护	厦门服云	魅影 V2	10.198.12.3	1	哈尔滨 B02 资源池
主机防护	上海观安	魅影 V2	10.193.113.27	1	哈尔滨 B02 资源池
漏扫系统	启明	天镜	10.198.13.134	1	哈尔滨 B02 资源池
WAF	迪普	WAF3000-T A-C	10.198.1.22	1	哈尔滨 B02 资源池
APT	绿盟	NTANX3-YD 6100D-主	10.198.1.24	1	哈尔滨 B02 资源池
APT	绿盟	NTANX3-YD 6100D-探	10.198.1.25	1	哈尔滨 B02 资源池
APT	绿盟	TACNX3-D6 00A-沙箱	10.198.1.26	1	哈尔滨 B02 资源池
入侵检测	天融信	TI-96434	10.198.1.23	1	哈尔滨 B02 资源池
APT	亚信	UAP	10.139.151.11	1	哈尔滨 B14 资源池
蜜罐	上海观安	魅影 V2	10.232.152.134	1	哈尔滨 B14 资源池
蜜罐	上海观安	魅影 V2	10.232.152.139	1	哈尔滨 B14 资源池
蜜罐	上海观安	魅影 V2	10.232.152.133	1	哈尔滨 B14 资源池
抗 DDOS	迪普	DPtech UMC 统一	10.193.113.25	1	哈尔滨 B02 资源池
入侵检测	中科全安	全安网站 入侵检测	192.168.108.106	1	哈尔滨 B02 资源池
入侵检测	中科全安	全安网站 入侵检测	10.192.1.21	1	哈尔滨 B02 资源池

入侵检测	中科全安	全安网站 入侵检测 系统	10.192.65.21	1	哈尔滨 B02 资源池
------	------	--------------------	--------------	---	-------------

1.3.4 网络边界

经营分析系统隶属于大数据平台，对内通过集团内层防火墙与核心网隔离，进行安全访问控制，对外边界部署了抗 DDOS、蜜罐、入侵检测等安全设备，实现网络安全隔离与入侵检测防护等。

2 中国移动通信集团吉林有限公司信息技术部经营分析系统安全等级的确定

2.1 安全等级定级计算方法

根据网络单元的社会影响力I、规模和服务范围R、所提供服务重要性V三个定级要素的赋值，采用以下公式来计算网络单元的安全等级值：

$$k = \text{Round1} \{ \text{Log}_2 [\alpha \times 2^I + \beta \times 2^R + \gamma \times 2^V] \}$$

其中，k代表安全等级值，I代表社会影响力赋值、R代表规模和服务范围赋值、V代表所提供服务的的重要性赋值，Round1{}表示四舍五入处理，保留1位小数，Log2[]表示取以2为底的对数， α 、 β 、 γ 分别表示网络单元的社会影响力、规模和服务范围、所提供服务的的重要性赋值所占的权重，分别为1/3、1/3、1/3。

计算所得网络单元的安全等级值与安全等级的映射关系如下表所示。

表 安全等级值与安全等级的映射关系

安全等级值k	安全等级
$1 \leq k < 1.5$	第1级
$1.5 \leq k < 2.5$	第2级
$2.5 \leq k \leq 4$	第3级
$4 < k < 4.5$	第4级

$4.5 \leq k \leq 5$	第5级
---------------------	-----

2.1.1 社会影响力

社会影响力指标	赋值
网络/系统单元受到破坏后不损害国家安全、社会秩序、经济运行和公共利益	1
网络/系统单元受到破坏后不损害国家安全，对社会秩序、经济运行和公共利益造成轻微损害	2
网络/系统单元受到破坏后对国家安全造成较大损害，或者对社会秩序、经济运行和公共利益造成较为严重的损害	3
网络/系统单元受到破坏后对国家安全造成严重损害，或者对社会秩序、经济运行和公共利益造成特别严重损害	4
网络/系统单元受到破坏后对国家安全造成特别严重损害	5

简要说明：

中国移动通信集团吉林有限公司信息技术部经营分析系统为中国移动通信集团吉林有限公司信息技术部内部运营的平台，受到破坏后不损害国家安全，但是对社会秩序、经济运行和公共利益造成轻微损害，其社会影响力赋值应为 I=2。

2.1.2 规模和服务范围赋值

规模和服务范围指标	赋值
10 万用户以下	1
10 万（含）以上，200 万以下用户	2
200 万（含）以上，4000 万以下用户	3
4000 万（含）以上，1 亿以下用户	4
1 亿（含）以上用户	5

简要说明：

中国移动通信集团吉林有限公司信息技术部经营分析系统所服务的用户数为 10 万（含）以上，200 万以下，因此规模和服务范围 R=2。

2.1.3 提供服务的重要性赋值

所提供服务的的重要性指标	赋值
网络/系统单元所提供服务的的重要性较低，被破坏后对网络和业务运营商的合法权益造成轻微损害	1
网络/系统单元所提供服务的的重要性一般，被破坏后对网络和业务运营商的合法权益造成较大损害	2
网络/系统单元所提供服务的的重要性很高，被破坏后对网络和业务运营商的合法权益造成很大损害	3
网络/系统单元所提供服务的的重要性非常高，被破坏后对网络和业务运营商的合法权益造成非常大的损害	4
网络/系统单元所提供服务的的重要性特别高，被破坏后对网络和业务运营商的合法权益造成特别严重的损害	5

简要说明：

中国移动通信集团吉林有限公司信息技术部经营分析系统所提供服务的的重要性一般，当中国移动通信集团吉林有限公司信息技术部经营分析系统系统所提供服务的的重要性一般，被破坏后对网络和业务运营商的合法权益造成较大损害，其所提供服务的重要性赋值 $v=2$ 。

2.2 中国移动通信集团吉林有限公司信息技术部经营分析系统安全保护等级

根据上述计算，中国移动通信集团吉林有限公司信息技术部经营分析系统定级为 2 级。