

ICS 33.040

M 16



# 中华人民共和国通信行业标准

YD/T 2704-2014

---

## 电信信息服务的安全准则

Guidelines on security of the information service for  
telecommunication

2014-10-14 发布

2014-10-14 实施

---

中华人民共和国工业和信息化部 发布



## 前 言

本标准按照GB/T1.1-2009给出的规则起草。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：武汉邮电科学研究院、中国移动通信集团公司、国家计算机网络应急技术处理协调中心。

本标准主要起草人：桑梓勤、刘利军、黄元飞、刘 磊、田慧蓉。



# 电信信息服务的安全准则

## 1 范围

本标准规定电信运营商和服务提供商提供电信信息服务的安全准则，包括电信信息服务的分类，电信信息服务的安全目标、安全需求、安全机制以及安全协同问题。

本标准适用于提供电信信息服务时的运营商，也可供其他行业参考。

## 2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 5271.8-2001 信息技术 词汇 第8部分：安全

ITU-T Q.956.3 (95) 使用No.1数字用户信令系统(DSS1)的计费补充业务第3阶段描述：反向计费(REV)

## 3 术语、定义和缩略语

### 3.1 术语和定义

GB/T 5271.8-2001中的术语和定义适用于本标准，另外以下术语和定义也适用于本标准。

#### 3.1.1

基本电信业务 Basic Telecommunication Service

见ITU-T Q.956.3 (95)的3.3.1。

#### 3.1.2

信息化服务

一个以信息技术与高科技手段为生产和生活中出现的问题提供优质解决方案，或对有可能出现的问题进行评估、预测与防范的服务形式。

### 3.2 缩略语

下列缩略语适用于本文件。补充:IP\WLAN\IDC\IPTV\ISP\IT\ICP等.注意附录B中有很多缩略语。

## 4 电信信息服务分类

### 4.1 概述

电信信息服务是指通过固定网、移动网、互联网以及其它的电信基础设施直接向终端用户提供语音信息服务、数据服务或在线信息和数据检索等信息服务，或为其它政府机构、企事业单位进行信息化建设提供服务。为了实现这一目标，电信运营商或其它第三方必须进行信息收集、开发和处理，并建立信息平台，使用户最终获得信息。

电信信息服务可分为三类，如图1所示。

——通信服务；

- 内容服务；
- 信息化服务。

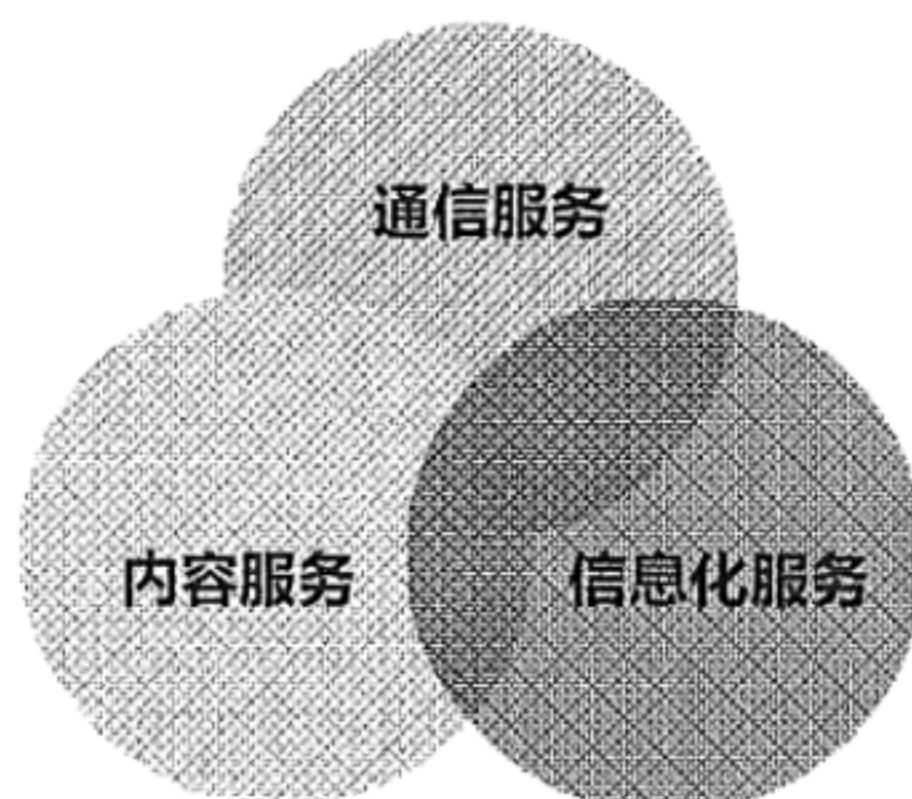


图1 电信信息服务分类

#### 4.2 通信服务

通信服务是运营商的传统业务，它通过网络基础设施（如固定通信网络、移动通信网络、互联网、卫星等）提供。业务的表现形式为语音、数据、多媒体和视频，即基本电信业务。典型服务包括：

- 电话业务；
- 互联网宽带服务；
- 无线市话；
- 号码查询；
- 即时通信（如飞信）；
- 可视电话。

#### 4.3 内容服务

内容服务是通信服务的扩展，它有可能是第三方如ISP或ICP提供的，也有可能是运营商自己提供的。典型的内容服务有：

- 接入门户；
- 互联网索引/搜索；
- 软件应用商店（如中国移动 Mobile Market、苹果 App Store 以及谷歌 Android Market 等）；
- 手机报/移动阅读/广告/新闻；
- 手机游戏/手机视频/移动电视/IPTV；
- 位置服务/移动导航；
- 电子彩票/手机证券；
- 手机支付/手机钱包；
- 远程教育/远程医疗。

通常情况下，运营商通过自营业务提供以上内容服务，或者通过其它公司获得音乐、电视、支付卡、股票交易等内容服务。第三方的内容也可通过运营商的网络传送给终端用户。



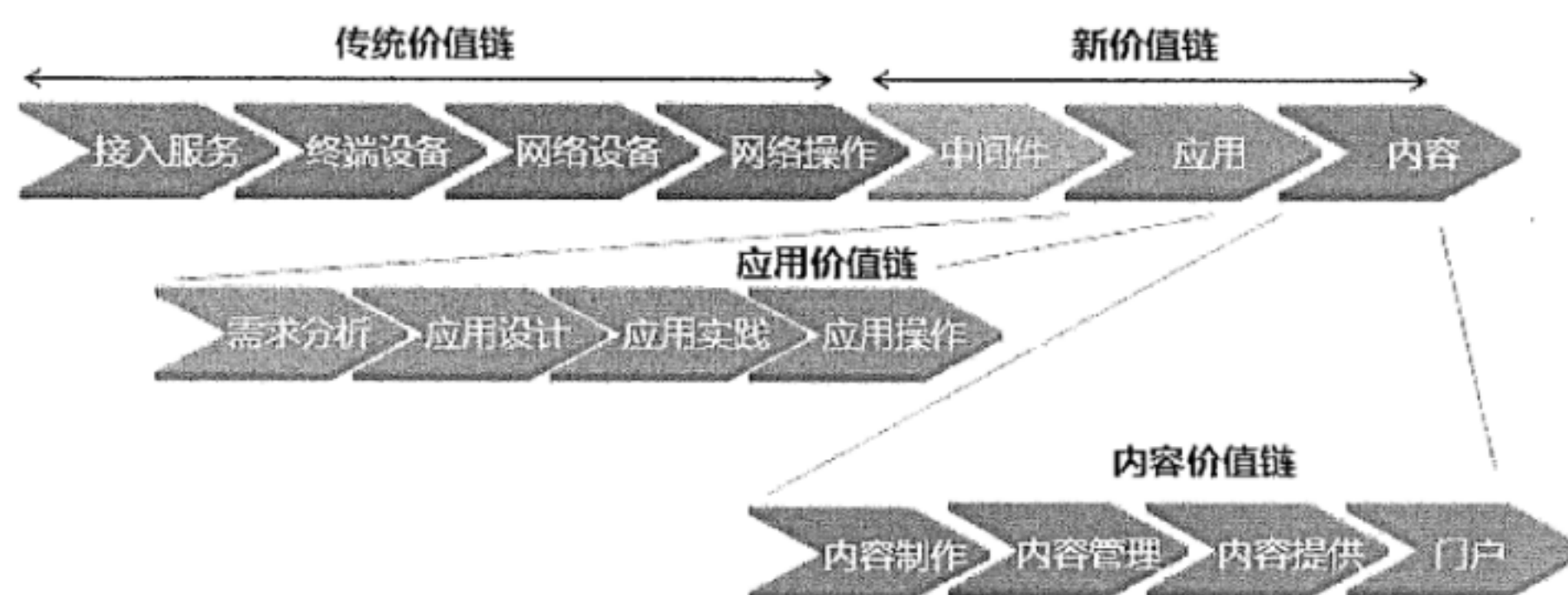


图2 内容服务

#### 4.4 信息化服务

信息化是信息社会的目标，电信运营商利用他们的网络资源与IT经验优势逐渐进入此领域，为生产和生活中出现的问题提供优质解决方案，或对有可能出现的问题进行评估、预测与防范，并提供与信息相关的咨询、培训、服务外包等。典型业务有：

- 办公自动化/企业邮箱/移动办公；
- 电子政务/电子商务/行业信息化（银行、制造业、交通物流等）；
- 视频监控；
- IDC 业务/企业建站/呼叫中心；
- 电子商务安全认证；
- 物联网/数字家庭。

#### 4.5 角色

电信信息服务的相关方有监管部门、运营商、第三方服务提供商和最终用户，在安全框架中，他们的角色和安全需求是不同的：

- 监管部门根据电信条例或法规提出安全要求，以保证业务的可用性，不同运营商之间进行公平竞争，保护用户的隐私；
- 运营商需要通过安全措施保护网络基础设施、正常运维以及自身的商业利益，需要对国内外用户和公众尽到职责；
- 第三方服务提供商需要通过安全措施保证他们的业务通过运营商的公众网络传送到最终用户；
- 最终用户在接受服务时需要保证机密性，包括业务的可用性和隐私保护。最终用户又分为集团用户和个人用户。运营商可采用不同的策略为不同的用户服务，即提供个性化的服务或差异化的服务。通常情况下，服务解决方案是按用户组来进行设计的，安全解决方案也是如此。

### 5 安全目标

安全目标是指提供电信信息服务时采取的安全措施所达到的目标，它的要点是：

- 只有合法用户才能使用运营商或第三方服务提供商提供的电信信息服务；用户的使用本身也是合法的/合乎要求的；
- 运营商或第三方服务提供商在用户使用电信信息业务时为用户提供隐私保护；
- 为了保证可用性和业务的连续性，运营商一方面防止用户未经请求而访问，另一方面保证第三

方的业务被安全地送达；

- 对安全事件可控，或者恢复正常状态，或者能把损失减到最小；
- 所施加的安全措施和机制不能影响业务质量，应综合考虑性能、可用性、可升级、成本代价；
- 只有经授权的运营商、业务提供商和用户才能在授权的范围内检索与之相关的电信信息服务的安全信息。

## 6 安全需求

### 6.1 概述

电信信息服务的安全需求主要解决以下几方面问题：

- 保密性（存储或传送信息时的保密性）；
- 数据完整性（保护存储或传送的信息准确无误）；
- 可控性（任何实体都要负责它所发起的活动安全）；
- 可用性（任何合法的实体都能正确地使用它的业务）；
- 可恢复、可管理能力（任何违反安全措施的活动都能被处理，恢复正常状态）。

### 6.2 通信服务的安全需求

传统电信服务在向信息服务转型过程中，服务内容的增加带来了新的安全问题。例如114查号服务变为个人总机或企业总机后，需要解决个人信息的隐私保护问题。又比如，为了提高信息服务质量方便用户，需要采用新的用户身份认证技术，如通过电话进行语音识别以及通过手机验证码查询账单等。因此即便是非常传统的电信业务，在进行业务拓展时也会带来前所未有的安全问题，从而有采用安全新技术的需求。

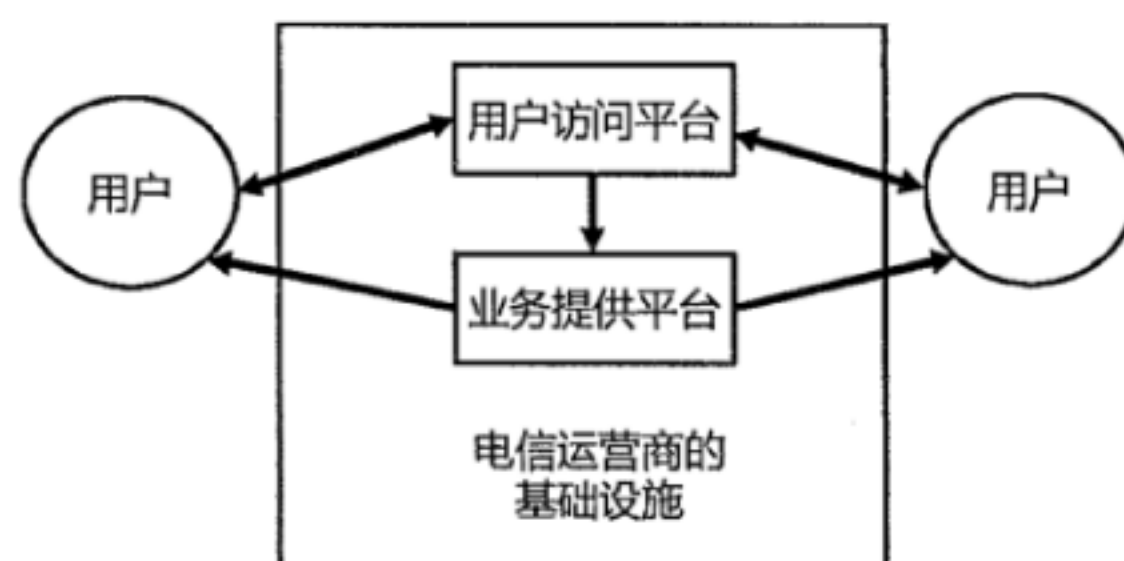


图3 通信服务模型

不同角色对通信服务的安全需求如下。

- 监管部门对于传统通信服务的安全需求：
  - 根据等级保护制度，对网络环境和服务开展安全定级、安全评测和风险评估；
  - 维护运营商之间公平的商业竞争关系；
  - 避免用户使用电信信息服务时产生的违法的行为和言论。
  - 监控用户在使用电信信息服务时的异常行为，对产生的违法行为和言论进行警示，控制不良后果，并配合主管部门追查责任。
- 运营商对于传统通信服务的安全需求：
  - 保证网络基础设施的持续稳定运转；
  - 确保用户的合法身份，防止非法用户使用服务；



- 确保用户操作合法，防止用户非法使用各类服务；
- 防止攻击者的恶意攻击行为，确保服务的可用性；
- 根据执法部门的要求，提供执法监听服务；
- 确保服务的容灾能力，能够应对一定程度的异常，迅速恢复并提供持续服务；
- 防止服务范围内重要信息被攻击者主动窃取或者被动泄露。

——用户对于传统通信服务的安全需求：

- 用户能够无障碍的合法使用权限内的服务；
- 用户的个人信息尤其是隐私部分不会被泄露或者窃取。

### 6.3 内容服务的安全需求

内容服务主要来源于互联网、广播电视等新业务，它包括电子商务、网络搜索、导航定位、通过电信网络传输的视频节目、数字地面广播等，涉及到信息内容审计、用户身份认证、客户资源管理等技术，同样也有安全需求。

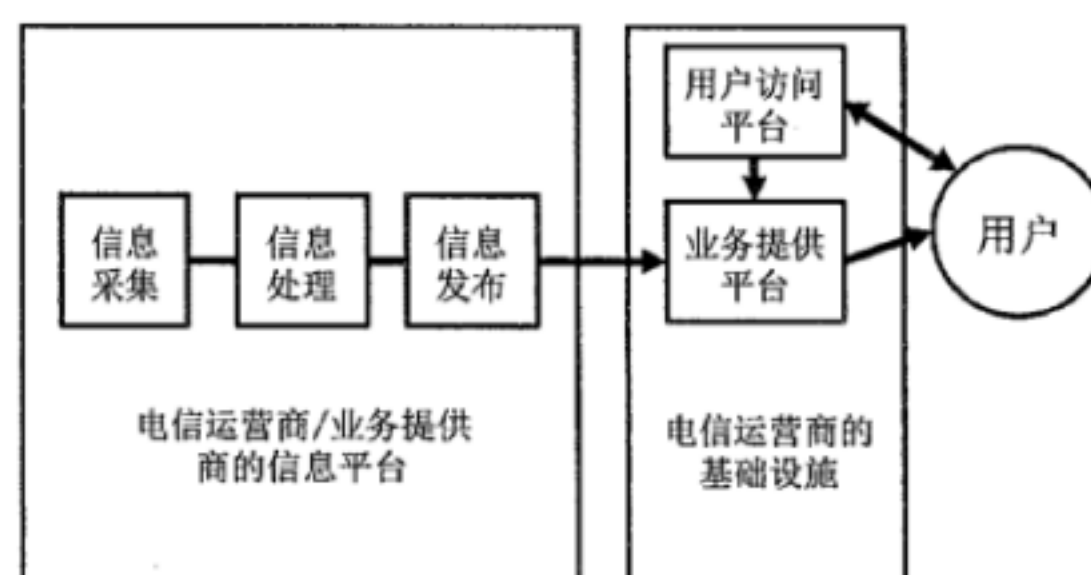


图4 第三方内容服务模型

不同角色对内容服务的安全需求如下。

——监管部门对于内容服务的安全需求：

- 维护运营商以及第三方服务提供商之间公平的商业竞争关系；
- 避免第三方服务提供商向公众发布非法、虚假或者不健康的信息和服务；
- 避免用户使用电信信息服务时产生的违法的行为和言论。
- 监控用户在使用电信信息服务时的异常行为，对产生的违法行为和言论进行警示，控制不良后果，

并配合主管部门追查责任。

——运营商对于内容服务的安全需求：

- 确保服务的可用性，尤其是某些实时服务的不间断性；
- 确保用户的合法身份，以及用户操作的合法性；
- 防止攻击者的恶意攻击行为，尤其是涉及到用户个人财产的攻击行为；
- 确保服务的容灾能力，能够应对一定程度的异常，迅速恢复并提供持续服务；
- 防止服务范围内重要信息被攻击者主动窃取或者被动泄露；
- 根据执法部门的要求，提供执法监听服务。

——第三方服务提供商对于内容服务的安全需求：

- 确保提供的信息的可用性，安全到达客户端，确保服务与客户的正常交互；
- 确保信息的完整性，不被篡改或者丢失；
- 确保提供的服务或者信息不被非法窃取或者泄露。

——用户对于内容服务的安全需求:

- 内容服务的用户主要是个人用户, 关注的是服务的可用性和隐私信息的安全性;
- 用户的服务尤其是收费服务持续稳定可用;
- 保证个人信息, 尤其是包括银行账号等在内的隐私信息不被非法访问或泄露;
- 要求尽可能避免服务的异常中断对于用户个人利益的损失。

#### 6.4 信息化服务的安全需求

针对政府/企业的信息化服务, 包括为政府/企业提供邮箱、数据存储、办公系统、网络IT规划与咨询等, 它一方面涉及到政府/企业的业务流程, 另一方面也涉及到政府/企业的商业秘密与技术秘密, 需要提供安全保护。

不同角色对信息化服务的安全需求如下。

——监管部门对于信息化服务的安全需求:

- 维护运营商之间公平的商业竞争关系;
- 根据信息安全等级保护制度保障机密信息包括商业秘密、技术秘密等的安全性;
- 避免用户使用电信信息服务时产生的违法的行为和言论。
- 监控用户在使用电信信息服务时的异常行为, 对产生的违法行为和言论进行警示, 控制不良后果, 并配合主管部门追查责任。

——运营商对于信息化服务的安全需求:

- 确保服务的可用性, 以不影响用户的正常办公/商务流程为准;
- 确保用户的合法身份, 以及用户操作的合法性;
- 防止攻击者的恶意攻击行为, 尤其是涉及金融行业的恶意攻击;
- 确保服务的容灾能力, 能够应对一定程度的异常, 迅速恢复并提供持续服务;
- 防止服务范围内重要信息被攻击者主动窃取或者被动泄露。

——第三方服务提供商对于信息化服务的安全需求:

- 确保服务中所包含信息的完整性和可用性;
- 确保提供的服务或者信息不被非法窃取或者泄露。

——用户对于信息化服务的安全需求:

- 信息化服务的用户主要是包括政府、企业在内的集团用户, 关注的是业务流程各环节的可用性和国家、商业、技术机密的保密性;
- 集团用户的服务要求稳定可用, 不影响业务流程, 业务中各关键环节不能异常或者中断服务;
- 实时的业务需要有较强的容灾性, 能够实时的切换到备用系统中, 不给企业造成损失;
- 保证政府和企业的商业机密、技术机密不被非法访问或者窃取。

#### 6.5 安全协同

个人用户是个性化信息服务的最基本单元, 集团用户是这些最基本单元的组合, 存在个人用户的信息安全保护与集团用户的信息安全保护的协同问题。需要满足以下机制:

——个人用户的安全策略应该建立在集团整体安全策略基础上, 即个人用户必须执行集团的安全策略, 比如个人需要安装或者更新所属集团统一部署的安全补丁和防病毒软件。

——当个体因特殊业务需求导致安全需求与集团安全策略冲突时, 需要根据实际情况采取措施并备案。



——集团中个体出现安全漏洞或者被攻击时，应告知集团安全管理员，为此所新增的防范措施需要统一部署到集团整体环境中。

——当个体用户出现安全异常时，需要首先从集团网络环境中隔离，在完成安全评估和处理后方可重新连入集团网络环境。

——安全策略尽可能的放置在集团的服务器或者网关上，尽量减轻个人用户终端的负载。

## 7 安全机制

针对不同类型的信息服务，需要有不同的安全机制。安全机制根据对应的安全防范需求和解决的问题分为规章制度、数据备份、身份管理、访问控制、数据安全性管理以及防范恶意攻击等6大类，表1给出针对三种不同信息服务类型所需的安全机制。

表1 安全机制列表

安全机制类型	安全机制条目	传统通信服务	内容服务	信息化服务
规章制度	制定行业法规规范商业行为，打击不正当经营和竞争	√	√	√
	根据等级保护制度进行安全定级和安全评测	√	√	√
数据备份	备份历史数据，用于安全事件调查和协助电子取证	语音信息	用户上网行为记录	行业数据
	灾备系统（包括网络、数据和服务器容灾），对于实时服务需要实时灾备	√	√	√
身份管理	对用户进行身份认证，包括口令、数字证书、短信验证码、数字移动证书、生物特征识别（语音识别、面部/虹膜/指纹识别）	口令 生物特征识别（主要是语音识别）	口令 数字证书 短信验证码 数字移动证书	口令 生物特征识别（主要是面部/虹膜/指纹识别）
访问控制	强制访问控制，根据等级保护制度定义访问规则	√根√根√根		
	自主访问控制，由服务或者信息的提供者规定访问规则	√由√由√由		
	基于角色的访问控制，设定角色、用户和权限	√于√于√于		
	信任管理，在跨域的环境里实现行为授权		√	√
数据安全性管理	用户数据加密，数据库加密，尽量避免信息的明文存储和传输	对用户身份信息加密	对用户身份信息加密，对用户在服务中的个人数据加密	重点对商业机密、科技机密和政府信息进行分级加密
	对网络流量进行监控和审计，过滤非法信息，内容审查	√	√网√	
防范恶意攻击	数据完整性校验	√	√	√
	企业版本的杀毒工具，防垃圾邮件			√
	对集团内部用户上网行为进行控制，避免感染病毒			√
	客户端防病毒软件	√	√	√
	服务器端的入侵检测系统	√	√	√
	对系统进行风险评估，通过系统加固和补丁升级方式减少系统漏洞	√	√	√
	运营商网关上的防火墙和防病毒软件	√	√	√

附 录 A

(资料性附录)

电信信息服务与增值电信业务的区别

YDN 126-2009定义了增值电信业务。从定义中可以看出，增值电信业务是一种附加通信业务，它使电信网络的经济效益或功能价值增高。

而电信信息服务是指通过信息采集、开发、处理和信息平台的建设，通过固定网、移动网或互联网等公众通信网络直接向终端用户提供语音信息服务或在线信息和数据检索等信息服务的业务，以及与信息化建议相关的信息服务。从这个定义可以看出，电信信息服务包括了原来的通信服务、内容服务和信息化建设服务。

## 附录 B

(资料性附录)

## 部分运营商的电信业务种类

## B.1 中国电信的电信业务

——电话业务：166 语音信箱业务、800 被叫集中付费业务、固网短信业务、来电显示业务、电话信息服务业务、17909 省内主叫直拨 IP 电话业务。

——数据通信业务：传真业务、数据通信业务。

——黄页信息业务：黄页信息咨询业务、网络类黄页业务、纸质类黄页电话号簿、黄页信息业务。

——融合业务：总机服务、综合办公、移动全球眼、手机对讲。

——互联网业务：电子彩票业务(17987)、电子信箱业务(E-MAIL)、电子商务证书业务(CTCA)、互联网数据中心(IDC)业务、WLAN 业务、LAN 业务。

——网元出租业务：设备出租业务、同步网端口出租业务、波长出租业务、通信光纤出租业务、管道出租业务、网元出租业务。

——国际及港澳台通信业务：国际及港澳台长途互联业务、国际及港澳台通信业务。

——应急通信业务：应急通信业务。

## B.2 中国移动的电信业务

——基本业务：国际漫游、国际长途、国内长途、国内漫游、本地通话。

——个人业务：

● 沟通：飞信、139 邮箱、号簿管家、短信回执、短信、彩信、语音信箱、来电提醒、主叫显示、呼叫转移、呼叫限制、主叫隐藏、可视电话、手机桌面助理。

● 商务：手机支付、手机钱包。

● 生活：12580、M-ZONE 淘乐汇、手机医疗、MO 手机上网、随 E 行、WLAN、随 e 行 G3 上网笔记本、无线上网、手机导航、移动搜索、手机视频、视频留言。

● 行业：手机证券、手机商界。

● 学习：手机报、手机阅读、快讯。

● 娱乐：彩铃、无线音乐俱乐部、无线音乐排行榜、无线音乐搜索、音乐随身听、多媒体彩铃、全曲下载、手机游戏、手机动漫、百宝箱。

——集团业务：

● 基础通信：基础话音、无线商话、手机对讲(PoC)、会议电话、视频会议、专线服务、专网服务、固定宽带接入、无线宽带接入、集团 V 网、综合 V 网、融合通信(IMS)、IDC 数据中心、商务宝、集团短/彩信。

● 办公管理：集团通讯录、企业邮箱、手机邮箱、黑莓(有更标准的说法吗,这只是一个品牌)、移动办公、企业一卡通、移动财务。

● 营销服务：集团彩铃、移动总机、800 被叫付费电话、95105 呼叫中心、移动 400、企业建站、移动 CRM。

● 生产控制：物联网应用、视频监控、车务通。



- 行业解决方案：政府信息化、农业信息化、教育信息化、电力信息化、银行业信息化、交通物流业信息化、商贸行业信息化、制造业信息化。

- 集成服务：无线城市。

- 动力100业务包：通信动力、办公动力、营销动力。

### B.3 中国联通的电信业务

——综合信息业务：宽带商务、116114 电话导航、传媒信息业务

——移动电话业务：市话和长途通话、漫游、点对点短信、联通在信、炫铃、丽音、如意邮箱、彩信

——固定电话业务：固定电话、无线市话、集团电话、公用电话、交互式会议电话、灵通短信、4006 呼叫中心、悦铃、电话声讯、电话 Q 吧、来电显示、呼叫转移、呼叫等待、呼叫保持、三方通话、闹钟服务、语音信箱

——互联网接入与应用：宽带接入、家庭网关、WLAN、IDC、宽带我世界、E 盾

——数据通信及多媒体通信：ATM、FR、DDN、数字电路、IPLC（国际专用出租电路）、IP-VPN 等虚拟组网、网视机、可视电话、通信助理、宽视界、IPTV

——国际业务：语音、线路租用、互联网和创新数据服务、漫游业务

——ICT 及其他：ICT、网元出租业务、应急通信业务

### B.4 英国电信的电信业务

——IT 服务：IT 战略和整合、虚拟数据中心、主机托管服务、数据中心整合、机房出租。

——安全和风险管理：安全监控托管服务、托管防火墙服务、网络访问安全服务、安全移动办公、邮件安全服务、PKI 托管、入侵防御服务、善意黑客行为网络测试、日志留存托管服务、漏洞扫描托管服务、身份验证。

——客户关系管理：下一代联络中心、托管联络中心、全球呼入服务、Contact Centre OnPremise、虚拟化服务。

——移动服务：MobileXpress 服务、Lan 设备、与思科的统一移动融合服务、微软 OCS 移动服务。

——统一通信服务：统一通信视频、商务语音服务、Onevoice 全球 VPN、基于微软技术的 UCC 服务、托管 IP 电话、网络会议服务、视频会议服务。

——网络服务：AAI 解决方案持续性能管理服务、智能 VPN、混合 VPN、AAI 解决方案咨询审核服务、IP 地址管理、IT 运营服务、MPLS 服务、专线服务、企业级卫星宽带服务、卫星移动宽带服务、定制 VSAT、快速站点设置、托管 IP 电话、托管 LAN、新兴技术服务、融合 LAN、融合 LAN 服务、融合网络服务。

——针对不同行业的产品和服务：Onevoice 移动接入。



中华人民共和国  
通信行业标准  
电信信息服务的安全准则

YD/T 2704-2014

\*

人民邮电出版社出版发行  
北京市丰台区成寿寺路11号邮电出版大厦  
邮政编码：100164  
北京康利胶印厂印刷  
版权所有 不得翻印

\*

开本：880×1230 1/16 2016年12月第1版  
印张：1 2016年12月北京第1次印刷  
字数：25千字

15115·492

定价：15元

本书如有印装质量问题，请与本社联系 电话：(010)81055492