ICS 33.040
M 16

YD

中华人民共和国通信行业标准

YD/T 3165-2016

内容分发网络服务
信息安全管理系统技术要求

Technical standard of information security management system for contentdelivery networkservice

2016-07-11 发布　　2016-07-11 实施

中华人民共和国工业和信息化部　发布

目　　次

前　言

本标准按照 GB/T 1.1-2009 给出的规则起草。

本标准是“互联网信息安全管理技术手段”系列标准之一。本系列标准预计结构和名称如下：

1. 《互联网数据中心和互联网接入服务信息安全管理系统技术要求》
2. 《互联网数据中心和互联网接入服务信息安全管理系统接口规范》
3. 《互联网数据中心和互联网接入服务信息安全管理系统与接口测试方法》
4. 《内容分发网络服务信息安全管理系统技术要求》
5. 《内容分发网络服务信息安全管理系统接口规范》
6. 《内容分发网络服务信息安全管理系统与接口测试方法》
7. 《互联网资源协作服务信息安全管理系统技术要求》
8. 《互联网资源协作服务信息安全管理系统接口规范》
9. 《互联网资源协作服务信息安全管理系统与接口测试方法》

随着互联网各类业务和应用的发展，将不断补充和完善本系列的相关标准。

本标准按照GB/T 1.1-2009给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

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：中国信息通信研究院、恒安嘉新（北京）科技有限公司、网宿科技股份有限公司、北京蓝汛通信技术有限责任公司、阿里云计算有限公司。

本标准主要起草人：张昊星、柳　青、杨剑锋、吴振刚、魏　薇、杜　伟、景慧昀、钱　康、杨振雄、金　宇、张旭洲、周丽丽、李冠华、苗　琳、张峰晓、张　健、吴振永、余建展、许会荃、缪安娜、郭　岳、张慧珍。

内容分发网络服务
信息安全管理系统技术要求

1 范围

本标准规定了内容分发网络类服务相关信息安全管理技术手段的基本要求。

本标准适用于为互联网信息服务提供者提供包括但不限于网页加速、下载加速、流媒体加速等服务的 CDN 业务经营者所建设的业务信息安全管理系统。

2 规范性引用文件

下列文件对于本标准的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本标准。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

YD/T 1728-2008　　电信网和互联网安全防护管理指南

3 术语和定义

《电信业务分类目录》界定的术语和定义及下列术语和定义适用于本文件。

3.1

安全监管系统　Security Monitor Management System

电信管理部门依照国家法律法规授权建设的信息安全监管系统。

3.2

信息安全管理系统　Information Security Management System

业务经营者建设的符合本标准所规定信息安全管理系统要求的所有软、硬件系统的集合。该定义仅适用于本标准中所特指的内容分发网络业务信息安全管理系统。

3.3

内容分发网络　Content Delivery Network

增值电信业务，定义详见中华人民共和国电信条例附录《电信业务分类目录》。

3.4

互联网数据中心　Internetdatacenter

增值电信业务，定义详见中华人民共和国电信条例附录《电信业务分类目录》。

3.5

互联网接入服务　Internetservice Provider

增值电信业务，定义详见中华人民共和国电信条例附录《电信业务分类目录》。本标准中所有未指明的 ISP 均特指互联网接入服务。

3.6

互联网信息服务　Internet Content Provider

增值电信业务，定义详见中华人民共和国电信条例附录《电信业务分类目录》。

3.7

IDC 业务机房　The Room of IDC Service

IDC 业务经营者利用既有的互联网通信线路、带宽资源及辅助设施（如温湿度控制、除尘、消防、供配电、安防等），建立具有标准化电信级业务的环境和放置业务相关设备的场所。

3.8

ISP 业务节点　The Node of ISP Service

ISP 业务经营者利用接入服务器和相应的软硬件资源建立的、为客户提供接入互联网服务的业务节点。

3.9

业务客户　Customer

CDN 业务的客户，包括通过 CDN 服务商获得网页加速、下载加速、流媒体加速等服务的业务客户。

3.10

访问用户　Access User

访问使用 CDN 网络进行内容分发的有关网站和应用的外部用户。

3.11

源 IP、源端口　Source IP、Source Port

访问用户所使用的 IP 地址和端口。

3.12

目的 IP、目的端口　Destination IP、Destination Port

IDC/ISP 业务客户所使用的 IP 地址和端口。

3.13

加速域名　Speedup Domain

需要进行内容分发的网站或应用所使用的域名，即使用 CDN 加速服务的域名。

3.14

CDN 子网　CDN Sub-Net

CNAME（别名记录）的顶级域名。CNAME又称别名记录，即源站域名所使用的内容分发网络别名。

3.15

源站　Source Site

存储用户原始数据的主机。使用内容分发网络加速的内容从源站获取。

4　缩略语

下列缩略语适用于本文件。

CDN	Content Delivery Network	内容分发网络
FTP	File Transfer Protocol	文件传输协议
HTTP	Hypertext transfer Protocol	超文本传输协议
ICP	Internet Content Provider	互联网信息服务
IDC	Internet Data Center	互联网数据中心
ISP	Internet Service Provider	互联网服务提供商
IP	Internet Protocol	互联网协议

ISMI	Information Security Management Interface	信息安全管理接口
ISMS	Information Security Management System	信息安全管理系统
NAT	Network Address Translation	网络地址转换
POP3	Post Office Protocol-version 3	邮政协议-第 3 版
SMMS	Security Monitor Management System	安全监管系统
SMTP	Simple Mail Transfer Protocol	简单邮件传输协议
TCP	Transmission Control Protocol	传输控制协议
UDP	User Datagram Protocol	用户数据报协议
URL	Uniform Resource Locator	统一资源定位符
XLS	eXtensible Language Stylesheet	可扩展电子表格格式
XML	eXtensible Markup Language	可扩展标记语言

5 系统概述

CDN 信息安全管理系统（ISMS）是 CDN 业务经营者建设的具有基础数据管理、信息安全管理、访问日志管理、业务状态监测等功能的信息安全管理系统，以满足 CDN 业务经营者和电信管理部门的信息安全管理需求。

每个 CDN 业务经营者应建设一个统一的 ISMS，并与电信管理部门建设的安全监管系统（SMMS）通过信息安全管理接口（ISMI）进行通信，实现本标准规定的有关功能。

ISMS 与 SMMS 之间的关系如图 1 所示。

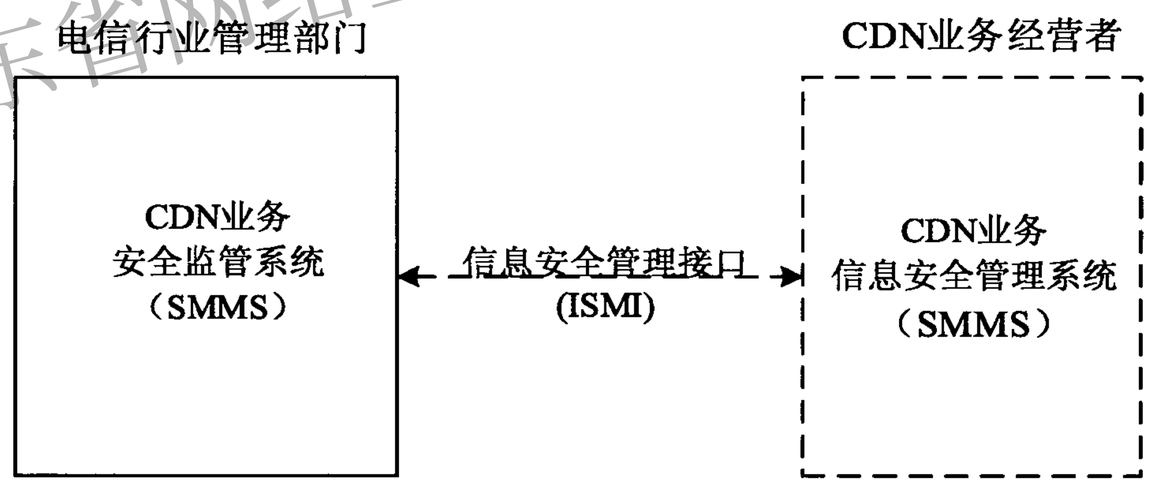

图 1 ISMS 与 SMMS 关系示意

本标准仅规定了 ISMS 功能和性能要求。ISMS 与 SMMS 之间的数据交换格式及通信方法，由《内容分发网络服务信息安全管理系统接口规范》另行规定。

6 系统功能

6.1 基础数据管理

6.1.1 基础数据的分类

ISMS 管理的 CDN 业务相关基础数据包括主体信息、资源信息两类。

a）主体信息包括 CDN 业务经营单位信息、CDN 业务客户信息。

1）CDN 业务经营单位信息包括 CDN 许可证号、单位名称（应与许可证上登记信息一致）、单位地址、企业法人、网络信息安全责任人信息，其中：

——网络信息安全负责任信息内容包括姓名，证件类型，证件号码，移动电话，固定电话。

2）客户信息包括客户编号、客户单位名称(或姓名)、客户单位属性、证件类型、证件号码、网络信息安全责任人信息、客户单位地址、应用服务信息，其中：

——应用服务信息内容包括预登记的服务内容、域名信息列表（对支持域名指向的应用服务等需提供本级域名），其中：

——域名信息包括加速域名、源站地址、备案或许可证号、顶级域名。

b）资源信息包括经营单位的 CDN 子网信息，包含 CDN 子网编号、CDN 子网顶级域名、CDN 子网顶级域名备案号、CDN 节点列表、CDN 节点信息、CDN 子网域名服务信息列表，其中：

1）CDN 节点信息包括 CDN 节点名称、CDN 节点机房信息。

CDN 节点机房信息包括占用机房信息、链路信息、机架信息、机房属性，IP 地址段信息，其中：

——占用机房信息包括占用机房名称、机房性质（租用需填写租用单位名）、机房所在省市、机房地址、接入厂商名称。

——链路信息包括 CDN 节点服务器使用的链路数量、链路带宽、链路类型及分配时间。

——机架信息，即 CDN 服务器在机房区域内使用的机架柜信息，主要包括：机架柜编码、所在机房区域、使用类型（自建/租用）。

——IP 地址段信息，包括 CDN 节点分配使用的 IP 地址段，含起始 IP 地址、终止 IP 地址、IP 地址使用方式（静态/动态）、IP 地址段序号。

2）CDN 子网域名服务信息包括域名编号，域名，域名源 IP，域名备案号，域名对应的顶级域名。

6.1.2 基础数据本地管理

ISMS 应实现基础数据的集中管理，包括基础数据本地存储以及有关数据本地进行增加、删除、修改等操作的功能。

ISMS 可支持采用 XML 或 XLS 等常见数据格式进行基础数据导入和导出。对于导入的数据，ISMS 应进行本地数据冲突校验，避免因导入数据可能出现的错漏与既有数据产生冲突。

6.1.3 基础数据上报与核验

ISMS 应能以业务经营者为单位，实现向 SMMS 上报基础数据的功能。对于客户信息，ISMS 只需上报业务客户编号、客户单位名称（或姓名）、应用服务信息列表。

ISMS 应具备基础数据信息更新后自动上报的功能，上报方式应为增量上报（即仅将新增或因修改存在变化的记录内容上报给 SMMS）。

ISMS 应支持 SMMS 对上报基础数据信息的校对与核验。对于经 SMMS 核验有误或存疑的退回记录，ISMS 应在收到后 24h 内进行补正并重新上报。

6.1.4 基础数据查询

ISMS 应能基于 SMMS 的基础数据信息查询指令，对本地记录进行检索并上报有关基础数据记录信息。

ISMS 应能基于 SMMS 的业务信息查询指令，对本地业务信息记录进行精确检索并实时上报相应的业务用户信息。ISMS 应支持的业务信息查询方式及输出要求见表 1。

表 1　客户信息查询方式

查询方式（查询条件）	查询输出要求（查询结果）
客户编号	该用户编号对应的业务客户信息，包括客户编号、客户单位名称(或姓名)、客户单位属性、证件类型、证件号码、网络信息安全责任人信息、客户单位地址、应用服务信息
业务许可证号	使用该域名的业务客户信息，包括客户编号、客户单位名称(或姓名)、客户单位属性、证件类型、证件号码、网络信息安全责任人信息、客户单位地址、应用服务信息
备案号	使用该域名的业务客户信息，包括客户编号、客户单位名称(或姓名)、客户单位属性、证件类型、证件号码、网络信息安全责任人信息、客户单位地址、应用服务信息
客户单位名称（或姓名）	使用该单位名称的业务用户信息，包括客户编号、客户单位名称(或姓名)、客户单位属性、证件类型、证件号码、网络信息安全责任人信息、客户单位地址、应用服务信息

6.2　业务状态监测

ISMS 应对 CDN 子网内有关业务链路上传送的公共信息数据进行全量监测，对使用 CDN 进行加速的活跃域名、活跃 IP 及应用端口等信息进行统计，形成业务状态监测记录。

业务状态监测记录应包括 CDN 子网内的活跃 IP 地址列表（含首次采集时间），CDN 子网内活跃域名列表（含首次采集时间、访问量、应用协议类型及数量）。

ISMS 应支持通过访问量对活跃域名列表进行排序，以反映相应资源的活跃程度。

业务状态监测记录应按日向 SMMS 上报，ISMS 至少应缓存有关监测记录直至完成向 SMMS 上报。

6.3　信息安全管理

6.3.1　违法违规网站管理

ISMS 应支持违法网站列表本地管理功能，并能接收 SMMS 下发的违法网站列表。

ISMS 应具备将加速域名与业务经营单位本地的网站备案记录或 ICP/IP 地址/域名信息备案库、违法网站列表等数据进行比对的方式，自动实现对未备案网站和违法违规网站的监测、处置等功能。

违法违规网站监测记录应包括违法违规网站的域名、IP、服务内容、违法违规情况、24h 累计访问量、记录时间（最后访问时间）。

违法违规网站监测记录上报周期为日，同时应按“零报告”的要求定时上报给 SMMS。

ISMS 应实现监测记录的本地存储功能，保存时间不少于 60 日，并供 SMMS 查询。

6.3.2　违法信息监测和处置

ISMS 应支持 SMMS 通过下发违法信息监测/过滤指令的方式，至少实现基于域名（包括使用特定域名的应用）、IP 地址（使用特定源/目的 IP 的数据包或会话）、源/目的端口（使用特定源/目的端口的数据包或会话）、传输层协议类型（TCP/UDP）、URL（使用包含特定字符串的 URL 所指向的资源）、关键词（页面标题和正文中含有特定明文关键词的页面，该功能为可选）规则的违法信息管理功能。

对 SMMS 下发的信息安全管理指令，分为管理指令与控制指令两种指令形式。管理指令由 SMMS 下发时，可以定义生效时间（过滤指令默认两个小时后生效），ISMS 接收到管理指令后 CDN 业务提供商根据实际业务情况可以在生效期限内向管理部门提出申诉，逾期则指令自动生效。如果提出申诉，ISMS 可暂停执行该指令直至收到 SMMS 的申诉反馈，如申诉成功则终止执行该指令，否则立即执行。执行控制指令由 SMMS 即时下发，即时生效。管理指令适用范围包括所有类型的信息安全管理指令，控制指令的适用范围仅限于违法信息过滤指令。

ISMS 应能对所有符合违法信息监测规则的 TCP 和 UDP 协议流量进行监测，应至少能对符合违法信息过滤规则的 TCP 协议流量进行过滤处置。

ISMS 应确保在信息安全指令管理功能的实现过程中，按照 SMMS 下发指令的优先级高于 ISMS 本地指令、过滤指令的优先级高于监测指令的原则，根据相关指令的优先级实现规则冲突校验和提醒功能。对于同类指令中规则内容有包含关系的按优先级执行（如域名过滤与该域名下 URL 过滤指令同时下发时，优先执行域名过滤指令）。

对于生效的违法信息监测/过滤指令应生成相应的违法信息监测/过滤记录，记录内容包括源/目的 IP，源/目的端口、违法信息、首次触发时间、最近触发时间、触发指令次数以及触发的指令标识，对浏览类应用还需记录 URL。

对于页面标题或正文含有违法信息监测/过滤规则指定关键词的页面（该功能为可选实现），ISMS 应在当日的首次监测/过滤记录保存相应页面的纯文本页面快照（页面缓存）。

对于生效的违法信息监测、过滤指令，ISMS 至少应缓存有关监测、过滤记录直至完成向 SMMS 上报。

对于生效的违法信息监测、过滤指令，应实时或定期（不超过 2h）将对应的监测、过滤记录上报至 SMMS，且上报完成时间不得超过 4h。对于过滤指令未生成过滤记录的，按“零报告”要求上报。

6.4 访问日志管理

6.4.1 访问日志记录功能

ISMS 应基于外部访问用户对使用 CDN 进行加速的互联网信息服务业务客户有关应用和服务的成功访问行为，完整记录和统计访问信息，形成访问日志。

——对于可通过传输层协议或应用层协议头信息区分会话特征的数据流量，ISMS 应以会话为单位记录访问日志，记录信息至少应包括源 IP、目的 IP、源端口、目的端口、访问时间（起始时间，精确到秒），属于浏览类协议的访问需留存 URL。

——对于采用加密方式的会话，记录的访问日志应至少包括源 IP、目的 IP、源端口、目的端口、访问时间（起始时间，精确到秒）。

——对于无法通过传输层协议或应用层协议报文头内容区分会话特征的数据流量，ISMS 应以数据流（源 IP、目的 IP、源端口、目的端口均相同，速率大于 1 帧/秒且持续时间>10s 的数据流量）为单位记录访问日志，记录信息至少应包括源 IP、目的 IP、源端口、目的端口、访问时间（起始时间，精确到秒）、持续时长（精确到秒）。

6.4.2 日志记录查询方式

ISMS 应支持 SMMS 对访问日志记录全部字段内容的精确查询、检索功能。

ISMS 应支持的访问日志查询方式见表 2。其中，“M”为必须支持，“O”为可选支持。

表 2 日志留存查询方式

日志留存查询方式	属性	查询结果
源IP地址、查询时间	M	6.3.3节a）
源IP地址、目的IP地址、查询时间	M	6.3.3节b）
源IP地址、用户访问URL、查询时间	M	6.3.3节c）
源IP地址、用户访问URL、目的IP地址、查询时间	O	6.3.3节d）
目的IP地址、查询时间	M	6.3.3节e）
用户访问URL、查询时间	M	6.3.3节f）
目的IP地址、用户访问URL、查询时间	O	6.3.3节g）
注：查询时间指明确起止时间点的查询时段（单次查询的时间跨度以不大于3min为宜）		

6.4.3 日志记录查询结果

ISMS 向 SMMS 返回的访问日志记录查询结果应符合如下要求：

a）源 IP 地址+查询时间

依据源 IP 地址及查询时间，ISMS 应至少上报目的 IP 地址、目的端口、用户访问 URL、访问时间。

查询响应指标应符合：查询时间跨度不超过 30min，应在 2h 内完成查询结果上报。

b）源 IP 地址+目的 IP 地址+查询时间

依据源 IP 地址、目的 IP 地址及查询时间，ISMS 应至少上报用户访问 URL、源端口、目的端口、访问时间。

查询响应指标应符合：查询时间跨度不超过 30min，应在 1h 内完成查询结果上报。

c）源 IP 地址+用户访问 URL+查询时间

依据源 IP 地址、用户访问 URL 及查询时间，ISMS 应至少上报目的 IP 地址、目的端口、源端口、访问时间。

查询响应指标应符合：查询时间跨度不超过 30min，应在 1h 内完成查询结果上报。

d）源 IP 地址、用户访问 URL、目的 IP 地址、查询时间

依据源 IP 地址、目的 IP 地址、用户访问 URL 及查询时间，ISMS 应至少上报：目的端口、源端口、访问时间。

查询响应指标应符合：查询时间跨度不超过 30min，应在 1h 内完成查询结果上报。

e）目的 IP 地址、查询时间

依据目的 IP 地址及查询时间，ISMS 应至少上报：源 IP 地址、目的端口、用户访问 URL、访问时间。

查询响应指标应符合：查询时间跨度不超过 30min，应在 1h 内完成查询结果上报。

f）用户访问 URL、查询时间

依据用户访问 URL 及查询时间，ISMS 应至少上报：源 IP 地址、目的端口、目的 IP 地址、访问时间。

查询响应指标应符合：查询时间跨度不超过 30min，应在 30min 内完成查询结果上报。

g）目的 IP 地址用户访问 URL、查询时间

依据用户访问 URL、目的 IP 地址及查询时间，ISMS 应至少上报：源 IP 地址、目的端口、访问时间。

查询响应指标应符合：查询时间跨度不超过 30min，应在 30min 内完成查询结果上报。

对于最近 60 日内的访问日志，应满足上述查询响应指标的要求。对于超过 60 日的访问日志，应在 24 小时之内完成查询结果上报。

6.4.4 日志留存时间

ISMS 所记录访问日志的保存时间应满足国家和行业主管部门所规定的要求。

6.5 系统功能管理

6.5.1 权限管理

ISMS 应实现对系统管理人员、操作人员、维护人员的身份认证和权限管理，根据不同的角色授予相应的权限，未经授权的用户不得使用 ISMS 的相应功能。

ISMS 应严格限制默认账号的权限，各账号应依据最小授权原则授予为完成各自承担任务所需的权限。

ISMS 应记录系统登录和操作日志，记录至少应包括登录/操作账号、时间、登录用户 IP 及操作内容等。

ISMS 应对 SMMS 下发指令及其执行状态进行有效保护，防止受到未授权的干扰与影响，且 ISMS 应能根据 SMMS 下发指令中的可读标记来实现 ISMS 侧全部用户对特定指令及其执行结果的权限控制。

6.5.2 运行维护

ISMS 应实现各子系统、组件程序的集中配置管理，对各系统、服务程序的运行状态进行实时监控，为系统的正常运行提供保障。

ISMS 应支持 SMMS 通过代码表发布指令的方式来实现在用数据代码的更新。

6.6 疑似数据与异常数据处置

ISMS 应支持对 SMMS 下发的疑似数据或异常数据信息的管理和处理反馈功能。其中：

——疑似数据为 SMMS 将其监测引擎所发现的 CDN 业务数据，在与 ISMS 上报的基础数据进行比对后不一致的数据，下发给 ISMS 进行核实。

——异常数据为 SMMS 将 ISMS 上报的基础数据与其业务状态监测上报的数据进行比对后不一致的数据，下发给 ISMS 进行核实。

ISMS 应在接收到 SMMS 下发的疑似数据或异常数据后一周之内，完成核实处理（对真实存在问题的疑似或异常数据重新上报或者整改，对核实后无误的数据进行反馈），并将处理后的情况上报给 SMMS。

7 通信接口

ISMS 应支持 ISMI 数据通信接口，接受 SMMS 下发的指令，完成基础数据与管理信息上报，并实现接口规范的管理功能。

8 性能要求

8.1 处理能力

ISMS 处理能力应不低于经营 CDN 业务的总链路带宽。

ISMS 应能对所覆盖的各 CDN 子网所使用的全部业务链路传送数据报文的关联和线速处理，避免对各类数据报文造成丢失或较大延迟等影响。

ISMS 应提供各类记录的快速查询手段，应能在接收 SMMS 各类查询指令后 10min 内返回查询结果（上文中已明确查询响应时间的除外）。

ISMS 应在基础数据更新后 10min 内将更新记录上报至 SMMS。

ISMS 应在收到 SMMS 下发的基础数据查询指令后实时将查询结果上报至 SMMS。ISMS 基础数据监测异常记录错漏比例应不高于 1%。

ISMS 应及时记录访问日志，应能在访问行为发生后 2h 内有效查询到相应的访问日志记录，且查询响应时间不大于 2h。访问日志记录错漏比例应不高于 1%，访问时间记录误差不大于 10s。

ISMS 支持的违法信息监测/过滤规则总数目至少应达到 5 万条。

ISMS 在所覆盖业务链路的峰值流量压力下，按 5 万条生效的违法信息监测规则（特定域名、特定

URL、特定关键词的规则至少各 1 万条）对违法信息实施监测的准确率不低于 95%、漏判及误判总量不高于 5%；按 5 万条生效的违法信息过滤规则（条件同前）对违法信息实施过滤的成功比例不低于 95%。

ISMS 应在各类记录上报 10min 内向 SMMS 查询数据接收及处理结果，及时解决数据处理过程中产生的错误和异常，并重新进行数据上报。

ISMS 业务状态监测记录访问量错漏比例应不高于 1%。

8.2 扩展能力

ISMS 应具备可扩展能力，可根据 CDN 子网及有关业务链路的变化及时进行平滑扩展。

8.3 可靠性

ISMS 系统可靠性应达到 99.99%以上，即 ISMS 系统及相关设备年宕机时间累计应不超过 0.88h。

ISMS 系统及相关设备运行或发生故障时，均应不影响 CDN 子网有关的正常业务和应用。

9 安全性要求

9.1 系统和数据安全

ISMS 相关操作、管理应提供并启用身份鉴别、标识唯一性检查、鉴别信息复杂度检查、及登录失败处理功能，保证系统中不存在重复用户身份标识，身份鉴别信息不易被冒用，并根据安全策略对登录失败可采取结束会话、限制非法登录次数和自动退出等措施。

ISMS 系统应提供覆盖到每个账号的安全审计功能，应保证无法删除、修改或覆盖审计记录。

ISMS 系统及相关设备应采取必要的管理和技术措施确保 ISMS 本身以及有关数据的安全，防止被非法访问和使用。

ISMS 系统的各类数据和日志信息应进行加密存储、传输，并采用消息认证等技术对系统传输数据进行处理，避免数据在传输过程中被非法截取。ISMS 与 SMMS 通信的双方应利用双向认证等技术，确保通信双方的正确身份和不可抵赖性。

ISMS 系统应对用户信息、业务数据等提供严格的本地访问控制机制，确保有关数据的授权访问。CDN 业务经营者对用户信息、日志信息等负有保密义务，不得违法使用 ISMS 记录的用户及日志信息。

ISMS 系统应对与外部交互数据的格式和内容进行合法性检测和过滤，防范可能利用系统接口功能缺陷的跨站和注入等攻击、入侵。

ISMS 系统及有关设备应遵循最小服务原则，仅开放必要的主机端口，应根据系统安全域防护策略启用访问控制功能，应在系统管理域边界处对可能的端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等攻击和入侵事件提供有效的抵御和防范能力。

ISMS 应提供可靠的系统数据备份与恢复功能。

ISMS 应按照 YD/T 1728-2008 及有关标准所确定的 3.1 级（或以上）安全防护要求进行系统安全设防。

9.2 时钟同步

ISMS 应保持所有服务器的时钟与国家标准时间同步，同步精度为秒，以保证系统时间、数据记录时间的准确性。

9.3 运行环境

ISMS 系统及相关设备应部署在安全可靠的运行环境中。

中华人民共和国
通信行业标准

内容分发网络服务
信息安全管理系统技术要求

YD/T 3165—2016

*

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

*

开本：880×1230　1/16　　2016 年 10 月第 1 版
印张：1　　2016 年 10 月北京第 1 次印刷
字数：23 千字

15115・1184
定价：15 元

本书如有印装质量问题，请与本社联系　电话：(010)81055492