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 1.1-2000 给出的规则起草。

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。

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

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

——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

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

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。

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

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

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