

ICS 33.040  
M 16

YD

# 中华人民共和国通信行业标准

YD/T 2405-XXXX  
替代YD/T 2405-2012

## 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

Interface standard of information security management system for  
Internet data center/Internet service provider

(送审稿)

××××-××-××发布

××××-××-××实施

中华人民共和国工业和信息化部 发布

## 目 次

目 次 .....	I
前 言 .....	III
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 缩略语 .....	1
5 概述 .....	1
6 接口功能要求 .....	2
6.1 基础数据管理 .....	2
6.2 访问日志管理 .....	3
6.3 信息安全管理 .....	3
6.4 代码表发布功能 .....	5
6.5 ISMS 状态报告功能 .....	6
7 接口流程 .....	6
7.1 通信方式 .....	6
7.2 管理指令处理流程 .....	6
7.3 查询指令处理流程 .....	7
7.4 数据上报流程 .....	8
8 接口方法定义 .....	9
8.1 idc_command()方法 .....	9
8.2 idc_commandack()方法 .....	11
8.3 file_load 方法 .....	13
9 编码说明 .....	14
9.1 互联网 IP 地址编码 .....	14
9.2 ICP 备案号 .....	14
10 数据代码表 .....	14
10.1 接入方式代码表 .....	14
10.2 单位属性代码表 .....	15
10.3 证件类型代码表 .....	15
10.4 机房性质代码表 .....	15
10.5 代理类型代码表 .....	15
10.6 服务内容代码表 .....	16
10.7 监测规则及过滤规则代码表 .....	16
10.8 违法违规情况表 .....	17
10.9 登记备案属性代码表 .....	17
10.10 指令优先级代码表 .....	17
11 数据交换内容描述 .....	18
11.1 数据格式及匹配要求 .....	18

11.2 基础数据查询指令内容 .....	18
11.3 基础数据上报内容 .....	19
11.4 基础数据监测数据上报内容 .....	26
11.5 访问日志查询指令内容 .....	27
11.6 访问日志查询结果上报内容 .....	28
11.7 违法信息安全管理指令内容 .....	28
11.8 违法信息监测记录上报内容 .....	30
11.9 违法信息过滤记录上报内容 .....	30
11.10 代码表发布指令内容 .....	31
11.11 指令执行情况上报内容 .....	32
11.12 ISMS 活动状态上报内容 .....	33
11.13 WebService 方法调用返回文件内容 .....	33
11.14 基础数据核验处理指令内容 .....	34
11.15 免过滤网站列表指令内容 .....	35
11.16 违法网站列表指令内容 .....	35
11.17 活跃资源监测数据上报内容 .....	35
11.18 违法违规网站监测数据上报内容 .....	37
11.19 活跃资源访问量查询指令内容 .....	37
11.20 违法管理指令执行记录指令 .....	37
附录 A （规范性附录） XML 文件格式定义 .....	错误！未定义书签。
A.1 file_load 方法 .....	错误！未定义书签。
A.2 基础数据查询指令 .....	错误！未定义书签。
A.3 基础数据上报 .....	错误！未定义书签。
A.4 基础数据监测异常数据上报 .....	错误！未定义书签。
A.5 访问日志查询指令 .....	错误！未定义书签。
A.6 访问日志查询结果上报 .....	错误！未定义书签。
A.7 违法信息安全管理指令 .....	错误！未定义书签。
A.8 信息安全管理指令执行情况上报 .....	错误！未定义书签。
A.9 违法信息监测记录上报 .....	错误！未定义书签。
A.10 违法信息过滤记录上报 .....	错误！未定义书签。
A.11 信息安全管理指令查询指令 .....	错误！未定义书签。
A.12 信息安全管理指令查询结果上报 .....	错误！未定义书签。
A.13 代码表发布指令 .....	错误！未定义书签。
A.14 WebService 方法调用返回 .....	错误！未定义书签。
A.15 ISMS 活动状态 .....	错误！未定义书签。
A.16 免过滤网站列表指令 .....	错误！未定义书签。
A.17 基础数据核验处理指令 .....	错误！未定义书签。
A.18 违法网站列表指令 .....	错误！未定义书签。
A.19 活跃资源监测上报 .....	错误！未定义书签。
A.20 违法违规网站监测数据 .....	错误！未定义书签。
A.21 指令执行情况上报文件格式描述 .....	错误！未定义书签。
A.22 活跃资源访问量查询指令 .....	错误！未定义书签。
A.23 违法管理指令执行记录指令 .....	错误！未定义书签。

## 前 言

本标准按照 GB/T 1.1-2009 给出的规则起草。

本标准是“互联网数据中心和互联网接入服务信息安全管理系统”系列标准之一，本系列标准的结构和名称如下：

- 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》（本标准）
- 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》

本标准代替 YD/T 2405-2012 《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》。本标准与 YD/T 2405-2012 相比，内容变化主要包括：

- 第 2、3、4 章中更新了本标准有关的规范性引用文件、术语和定义、缩略语；
- 第 6 章中更新和补充了基础数据核验处理、活跃资源监测/查询、违法网站/免过滤网站列表、核验处理等功能描述；
- 第 7 章中补充了数据上报和处理结果代码；
- 第 8 章中更新了接口方法有关参数和描述；
- 第 10 章中新增了指令优先级代码表，对不同指令的优先级别做出了规定；
- 第 11 章中删减了基础数据管理指令内容、信息安全管理指令内容、监测日志上报内容、过滤日志上报内容、信息安全管理指令查询指令内容、信息安全管理指令查询结果上报内容，补充和调整了基础数据查询指令内容、违法信息安全管理指令内容、违法信息监测/过滤记录上报内容、基础数据核验处理指令内容、免过滤网站列表指令内容、违法网站列表指令内容、活跃资源监测数据上报内容、违法违规网站监测数据上报内容、活跃资源访问量查询指令内容、违法管理指令执行记录指令内容等格式要求；
- 附录 A 中更新和补充了有关消息示例。

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：

本标准主要起草人：

本标准于 2012 年首次发布，本次为第一次修订。

# 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

### 1 范围

本标准规定了互联网数据中心和互联网接入服务类业务相关信息安全管理系统与电信管理部门依照国家法律法规授权建设的信息安全管理系统间接口的功能要求、数据通信要求及数据交换格式等。

本标准适用于提供包括但不限于业务机房及配套设施租赁、服务器托管和租用、虚拟主机等服务的 IDC 业务经营者及为互联网信息服务提供者提供互联网接入服务的 ISP 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。

GB/T 2260-2007 中华人民共和国行政区划代码

YD/T 2248 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

### 3 术语和定义

YD/T 2248 界定的术语和定义适用于本标准。

### 4 缩略语

下列缩略语适用于本标准。

FTP	File Transfer Protocol	文件传输协议
IDC	Internet Data Center	互联网数据中心
ICP	Internet Content Provider	互联网内容提供商
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
SMMS	Security Monitor Management System	安全监管系统
URL	Uniform Resource Locator	统一资源定位符
XML	Extensible Mark-up Language	可扩展标记语言

### 5 概述

IDC/ISP 信息安全管理系统接口（ISMI）是 IDC/ISP 企业侧信息安全管理系统（ISMS）与电信管理部门侧安全监管系统（SMMS）之间的接口，主要功能包括基础数据管理、访问日志管理、信息安全管理、代码表发布等。

ISMI 包括命令通道和数据通道。SMMS 通过命令通道下发指令给 ISMS，ISMS 通过数据通道上传数据给 SMMS。

ISMI 与 ISMS、SMMS 之间的关系如图 1 所示。

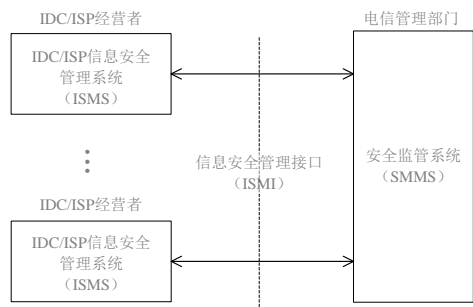


图 1 信息安全管理接口示意

每个 IDC/ISP 经营者应建设一个统一的 ISMS，并通过一个 ISMI 与 SMMS 对接，以实现对其所管辖范围内所有 IDC 业务机房/ISP 业务节点的管理。本标准中所有未指明的机房均泛指 IDC 业务机房或 ISP 业务节点。本标准仅规定了 ISMI 的功能要求、接口流程、接口方法及数据交换格式定义，ISMS 系统技术要求见 YD/T 2248。本标准中未明确的技术细节由 ISMS 根据 SMMS 的要求实现。SMMS 的技术要求不在本标准中规定。

6 接口功能要求

6.1 基础数据管理

基础数据管理包括基础数据上报与查询、基础数据异常监测，如图2所示。

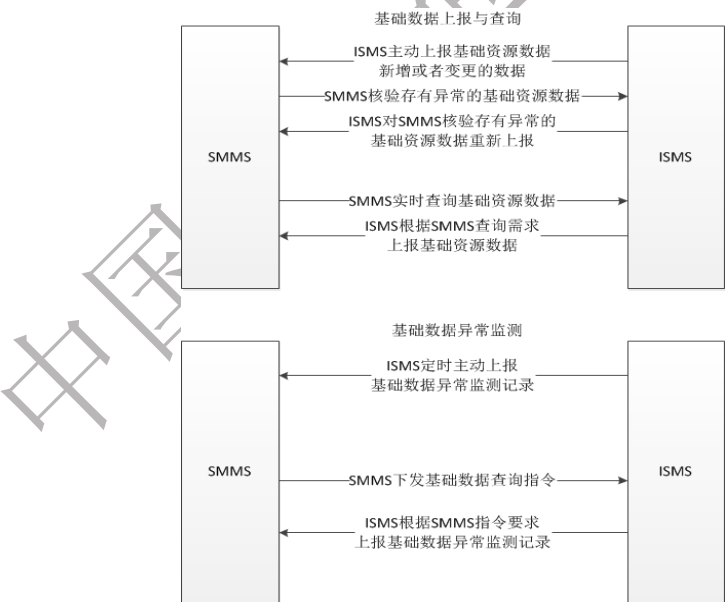


图 2 基础数据管理

——基础数据上报与查询

基础数据记录包括 IDC/ISP 经营单位、IDC/ISP 业务客户有关主体信息记录以及 IDC/ISP 业务经营单位所辖全部 IDC 业务机房/ISP 业务节点有关的资源信息记录。ISMS 应在本地新增基础数据或更新基础数据后同步将新增数据记录或含修改内容的数据记录上报给 SMMS，上报消息格式见 11.3 节。同时，ISMS 能根据 SMMS 的上报基础数据信息核验反馈指令，对存在异常的记录及时进行补正并重新上报，核验结果反馈消息格式见 11.14 节，上报消息格式见 11.3 节。

ISMS 应支持 SMMS 针对特定记录的实时查询。SMMS 通过 ISMI 接口向 ISMS 下发基础数据查询指令的方式实现基础数据查询。基础数据查询消息格式见 11.2 节、上报消息格式见 11.3 节。

——基础数据异常监测

ISMS 应对基础数据异常情况进行监测并形成基础数据监测异常记录。基础数据监测异常记录应定时通过 ISMI 自动上报并支持 SMMS 的实时查询。

SMMS 通过 ISMI 接口向 ISMS 下发基础数据查询指令的方式实现基础数据监测异常记录的查询功能，有关的基础数据监测异常记录的查询消息格式见 11.2 节，上报消息格式见 11.4 节。

6.2 访问日志管理

ISMS 应基于外部访问用户对 IDC/ISP 接入互联网业务客户有关应用和服务的访问行为，完整记录和统计访问信息，形成访问日志，并供 SMMS 查询，如图 3 所示。

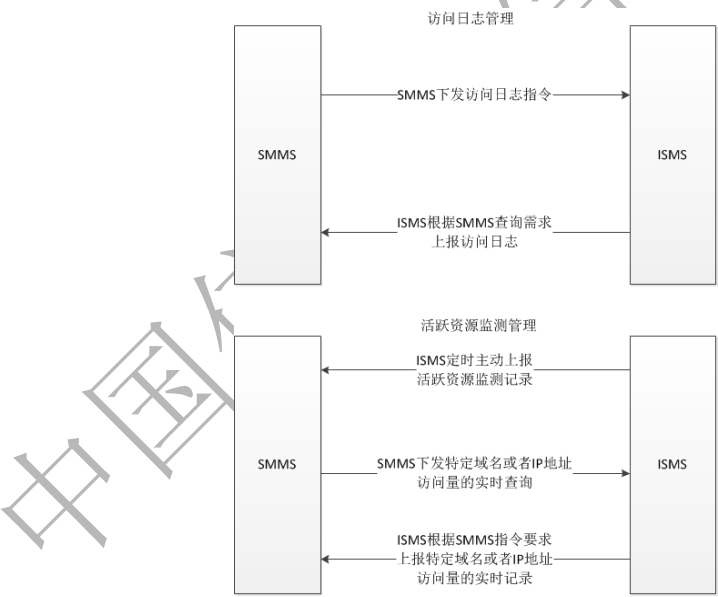
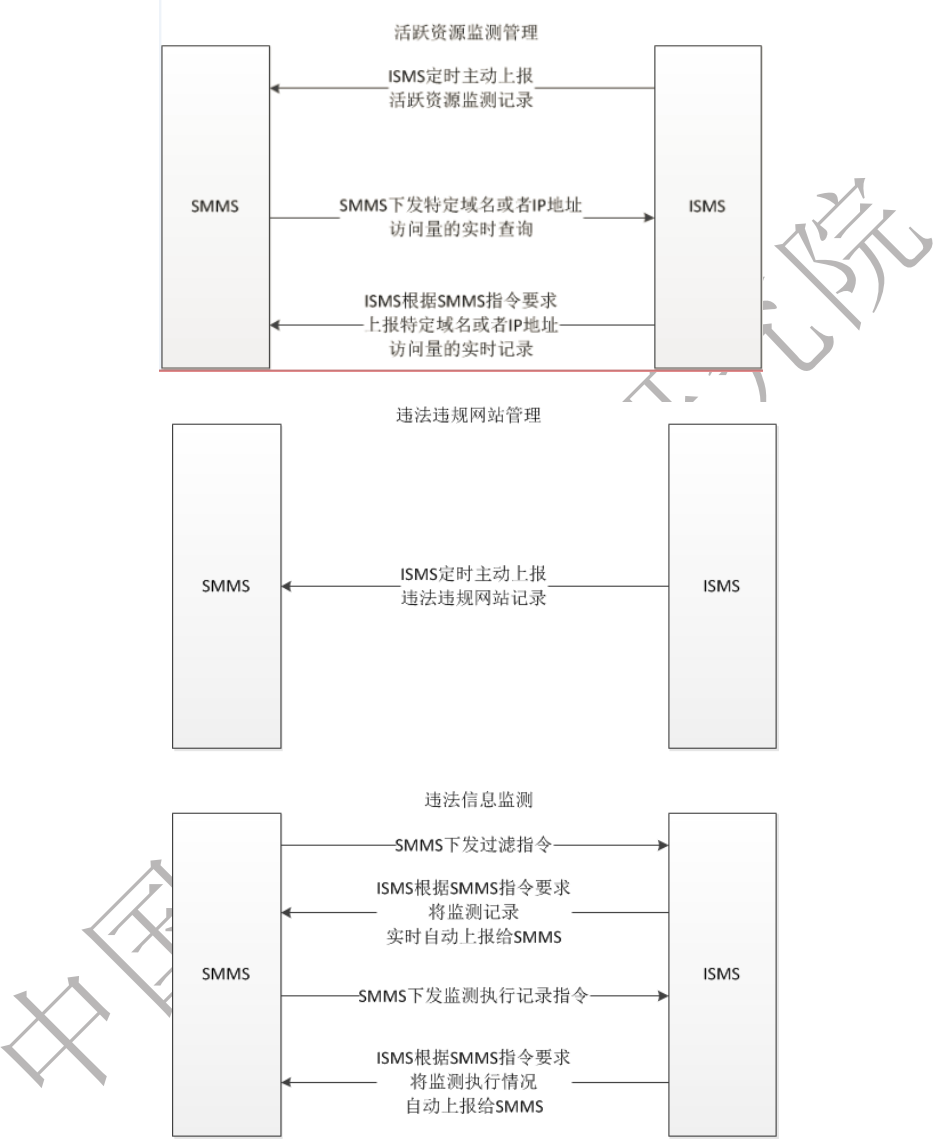


图 3 访问日志管理

SMMS 通过 ISMI 接口向 ISMS 下发访问日志查询指令的方式实现访问日志的查询功能，有关的访问日志查询消息格式见 11.5 节，上报消息格式见 11.6 节。

6.3 信息安全管理

SMMS 通过 ISMI 接口向 ISMS 下发信息安全管理指令和查询指令，实现活跃资源监测管理、违法违规网站管理、违法信息监测和处置等功能，如图 4 所示。





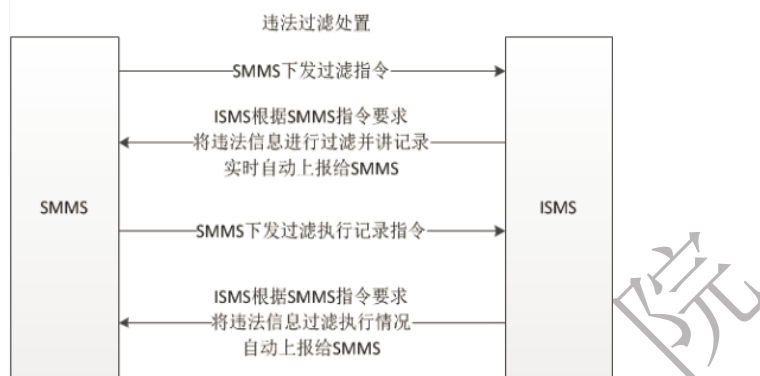


图 4 信息安全管理

——活跃资源监测管理功能：ISMS 应自动实现对机房内全部活跃域名、活跃 IP 地址访问量的监测和统计，并将记录信息主动定时上报给 SMMS。同时，ISMS 应支持 SMMS 针对特定域名和 IP 地址访问量的实时查询。有关上报消息格式见 11.17 节、查询消息格式见 11.19 节。

——违法违规网站管理功能：ISMS 应根据 SMMS 下发的违法网站列表实现违法违规网站发现和处置功能，对违法违规网站监测和处置情况进行记录。监测记录应定时通过 ISMI 自动上报并支持 SMMS 的实时查询。有关违法网站列表消息格式见 11.16 节、免过滤网站列表消息格式见 11.15 节、监测/处置记录上报消息格式见 11.4 节、查询消息格式见 11.20 节、管理指令执行情况上报消息格式见 11.11 节。

——违法信息监测功能：ISMS 应对 IDC/ISP 的双向流量数据进行监测，根据具体的违法信息监测指令对发现的违法信息进行记录。监测记录应实时通过 ISMI 自动上报并支持 SMMS 的查询。有关监测指令消息格式见 11.7 节，监测记录上报格式见 11.8 节，查询消息格式见 11.20 节，管理指令执行情况上报消息格式见 11.11 节。

——违法信息过滤处置功能：ISMS 应对 IDC/ISP 的双向流量数据进行监测，根据具体的违法信息过滤指令对发现的违法信息进行过滤处置，并进行记录。处置记录应实时通过 ISMI 自动上报并支持 SMMS 的查询。有关过滤处置指令消息格式见 11.7 节，过滤记录上报格式见 11.9 节，查询消息格式见 11.20 节，管理指令执行情况上报消息格式见 11.11 节。

#### 6.4 代码表发布功能

SMMS 通过代码表发布指令，将系统所用代码数据全量下发给 ISMS，ISMS 依据 SMMS 下发的代码，更新本地代码，如图 5 所示。有关的代码表发布消息格式见 11.10 节，指令执行情况上报消息格式见 11.11 节。



图 5 代码表发布功能

## 6.5 ISMS 状态报告功能

ISMS应每10min通过FTP方式向SMMS报告其状态信息，状态信息包括ISMS下级机房数目、出现异常的机房及对应机房ID，如图6所示。ISMS状态信息上报数据格式见11.12节。

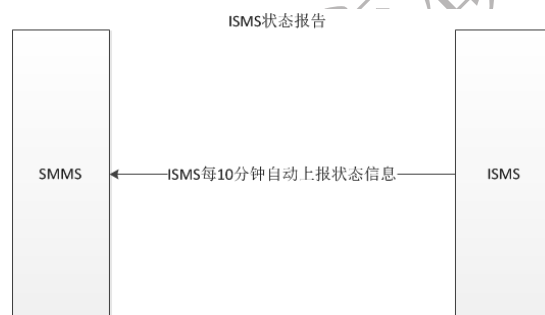


图 6 ISMS 状态报告功能

## 7 接口流程

### 7.1 通信方式

ISMI 包括命令通道和数据通道。

——命令通道采用 Webservice 方式，SMMS 通过调用 ISMI 接口方法将管理指令等下发给 ISMS，管理指令处理流程见 7.2 节，查询指令流程见 7.3 节，接口方法见 8.1 节、8.2 节；

——数据通道采用 FTP 方式，ISMS 使用 FTP 协议或 SFTP 协议将数据文件上报给 SMMS，数据上报流程见 7.4 节，接口方法见 8.3 节。

### 7.2 管理指令处理流程

SMMS 通过管理指令完成对 ISMS 基础数据核验处理、违法网站和免过滤网站列表管理、违法信息监测和处置指令管理以及代码更新管理等功能。SMMS 将管理指令发送到 ISMS 后，等待接收 ISMS 反馈的指令生效反馈信息。

管理指令处理流程如下（如图 7 所示）。

A.1 SMMS 系统调用 `idc_command()`方法，将指令下发至 ISMS。指令以 XML 文件的格式封装。

A.2 ISMS 接收 SMMS 下发指令，进行认证和信息校验，完成信息校验后保存指令，并在同一连接内及时反馈指令接收是否成功的信息（见 11.13 节）；如果 ISMS 没有成功收到下发命令，SMMS 则需要重新下发指令。

A.3 ISMS 在约定时间内执行指令，将指令生效的结果信息通过调用 `idc_commandack()`方法返回给 SMMS，返回的内容是以 XML 文件的格式封装的结果（见 11.11 节）。

A.4 SMMS 接收 ISMS 的指令生效结果信息，完成信息校验后进行保存，并在同一连接内及时反馈接收情况（见 11.13 节）；如 SMMS 没有成功收到指令生效信息，ISMS 需要重新上报指令生效结果信息。

A.5 如果下发的指令需要上报数据，则 ISMS 调用数据上报流程上报数据。

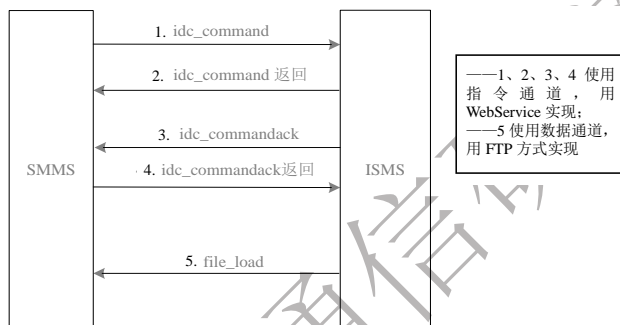


图 7 管理指令处理流程示意

### 7.3 查询指令处理流程

SMMS 通过查询指令查询 ISMS 的基础数据记录及其监测异常记录、访问日志记录、活跃资源监测记录、违法违规网站监测记录、违法信息监测和处置记录等。符合查询条件的数据记录通过数据上报流程异步上报到 SMMS。SMMS 按查询指令流程实现 ISMS 上报基础数据记录核验结果的反馈。

查询指令处理流程如下（如图 8 所示）。

- SMMS 系统调用 `idc_command()`方法，将查询指令下发至 ISMS。指令以 XML 文件的格式封装。
- ISMS 接收 SMMS 下发的查询指令，对指令进行信息校验。完成校验后保存查询指令，并在同一连接内及时反馈指令接收情况（见 11.13 节）；如 ISMS 没有成功接收到下发命令，SMMS 则需要重新下发。
- 查询的结果信息通过调用数据上报流程返回查询结果。

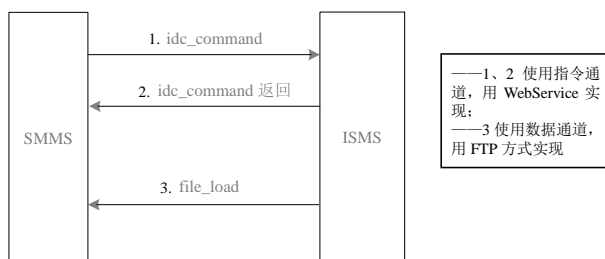


图 8 查询流程示意

#### 7.4 数据上报流程

数据上报流程中上报的数据包括基础数据记录、基础数据监测异常记录、访问日志记录、活跃资源监测记录、违法违规网站监测记录、违法信息监测和处置记录以及 ISMS 活动状态等。SMMS 为每个 ISMS 创建一个根目录，为便于描述，下文用 `idc_home` 表示该目录，ISMS 负责维护自己的根目录。

上报数据文件的存放路径规则为：`/idc_home/上报数据类型代码/上报日期/`。其中，上报数据类型共计 9 种，对应的代码见表 1，日期采用 `yyyy-MM-dd` 的格式编写。文件以生成时间命名且应带有 `.xml` 后缀名，生成时间用 1970 年 1 月 1 日到文件生成时的秒数表示（如，“生成时间.xml”形式）。

ISMS 通过数据通道，将上报的数据放到 SMMS 的相应目录下。数据上报文件大小的要求为单个上报数据文件必须小于 12M 字节，如上报数据量较大，可分拆为多个文件。

每个根目录下除了表 1 中所列的数据上报目录以外，还应有一个名为 999 的目录，用来存放 SMMS 生成的上报文件处理结果。特定上报文件的处理结果文件存放路径为：`/idc_home/999/数据类型代码-对应的文件原名-处理结果代码`。SMMS 生成数据上报处理结果为 UTF-8 编码的纯文本文件，文件内容为处理结果的必要描述，文件原名不含后缀（如，“上报数据类型代码-上报数据文件名-处理结果代码”形式）。其中，数据类型代码见表 1，处理结果代码见表 2。

表 1 数据上报类型代码表

代码	上报数据类型
1	基础数据记录
2	基础数据监测异常记录
3	访问日志查询记录
4	违法信息监测记录
5	违法信息过滤记录
6	（保留）
7	ISMS 活动状态
8	活跃资源监测记录
9	违法违规网站监测记录

表 2 上报文件处理结果代码

代码	上报数据类型
0	处理完成
1	文件解密失败
2	文件校验失败
3	文件解压缩失败
4	文件格式异常
5	文件内容异常（版本错误）
51	文件内容异常——上报类型错误
52	文件内容异常——节点/子节点长度错误
53	文件内容异常——节点/子节点类型错误
54	文件内容异常——节点/子节点内容错误
55	文件内容异常——节点/子节点缺漏
900	其他异常（存在其他错误，需重新上报）
999	其他异常（处理中）

每个 ISMS 在数据上报目录下有新建和写入权限，无删除权限；而在上报文件处理结果目录下有删除权限，无新建和写入权限。

数据上报的具体流程如下（如图 9 所示）。

- a) ISMS 产生上报数据并以 XML 文件的格式封装， ISMS 调用 file\_load 方法（见 8.3），将原始的上报数据经过压缩加密封装后仍以 XML 格式传送至 SMMS；
- b) SMMS 对上报的数据信息进行信息认证，如果认证成功则对上报的信息进行解密、解压等过程，得到原始上报数据，并进行相应处理；
- c) 处理结束后，SMMS 应生成相应的处理结果文件；
- d) ISMS 应在完成上报数据文件传送后及时获取 SMMS 对相应上报数据的处理结果，解决文件处理过程中产生的错误和异常，并重新进行数据上报流程。通常情况下，SMMS 对上报数据处理的时长不超过 10 分钟（如遇极端情况，SMMS 应在 10 分钟内通过代码“999”的处理结果文件告知 ISMS 相应上报数据仍在处理过程中）。

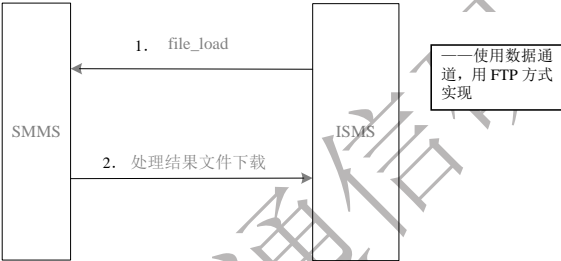


图 9 数据上报流程

8 接口方法定义

8.1 idc\_command()方法

8.1.1 方法原型

public String idc\_command (String idcId, String randVal, String pwdHash , String command, String commandHash, Int commandType, Long commandSequence, Int encryptAlgorithm, Int hashAlgorithm, Int compressionFormat, String commandVersion)。

8.1.2 服务请求地址

http://ISMS 服务器 IP 地址/IDCWebService/idcCommand?wsdl。

8.1.3 参数描述

本方法共使用 11 个参数，各项参数的描述如表 3 所示。

表 3 idc\_command () 方法参数

参数名称	参数类型	参数描述
idcId	字符串	IDC/ISP经营者ID，采用电信管理部门颁发的IDC/ISP许可证号，长度上限是18字节
randVal	字符串	SMMS调用该方法时生成的随机字符串，长度上限是20字节
pwdHash	字符串	将用户口令和随机字符串连接后使用hashAlgorithm指定的哈希算法进行哈希运算，然后进行base64编码得到的结果。 用户口令由设备所在SMMS维护管理，长度至少为6字节，最多32字节

command	字符串	对指令文件使用compressionFormat指定的压缩算法进行压缩，再对压缩后的信息按照encryptAlgorithm参数的要求进行加密，然后进行base64编码运算得到的结果； 指令包括基础数据查询指令（见11.2节）、基础数据核验处理指令（11.14节）、访问日志查询指令（见11.5节）、信息安全管理指令（见11.7节、11.15节、11.16节）、代码表发布指令（见11.10节）和信息安全查询指令（见11.18、11.19节、11.20节）
commandHash	字符串	对指令文件使用compressionFormat指定的压缩算法进行压缩，压缩后串接消息认证密钥，然后使用hashAlgorithm指定的哈希算法进行哈希运算得到哈希值，并对哈希值进行base64编码运算形成commandHash，用于验证完整性。 消息认证密钥由SMMS与ISMS事先配置确定，长度至少为20字节，最多32字节
commandType	整型	指令类型如下。 0：基础数据管理指令（基础数据核验处理指令）； 1：访问日志查询指令； 2：信息安全管理指令（违法网站列表管理指令、免过滤网站列表管理指令、违法信息监测和处置指令管理指令）； 3：保留 4：代码表发布指令 5：基础数据查询指令（基础数据记录查询指令、基础数据监测异常记录查询指令） 6：信息安全查询指令（活跃资源监测记录查询指令、违法违规网站监测记录查询指令、违法信息监测和处置记录查询指令）
commandSequence	长整型	本次指令下发的唯一编号
encryptAlgorithm	整型	对称加密算法。 0：不进行加密，明文传输； 1：AES加密算法。 加密密钥由SMMS与ISMS事先配置确定，长度至少为20字节，最多32字节。 ISMS应根据SMMS的要求完成加密算法的具体实现。ISMS至少应支持采用CBC模式、PKCS7Padding补码方式实现AES加密算法，并可根据SMMS的要求设置AES密钥长度、加密偏移量等参数。
hashAlgorithm	整型	哈希算法如下。 0：无hash； 1：MD5； 2：SHA-1； ISMS应根据SMMS的要求完成哈希算法的具体实现
compressionFormat	整型	压缩格式如下。 0：无压缩； 1：Zip压缩格式； ISMS应根据SMMS的要求完成压缩算法的具体实现
commandVersion	字符串	接口方法版本。符合本文件所规定要求的ISMI接口方法为“v2.0”，长度4字节

#### 8.1.4 方法描述

SMMS 调用该方法向 ISMS 下发管理指令、查询指令。SMMS 调用该接口方法下发指令时，同时完成认证和对指令文件的压缩加密处理。ISMS 指令文件认证和处理过程中哈希计算结果应采用十六进制字符串（英文字母小写）形式。

认证过程如下。

a) SMMS 产生长度上限为 20 的随机字符串（字符串由数字和大、小写字母构成），将该字符串与 SMMS 中存储的用户口令进行连接（例如，口令是字符串“1234567890”，生成的随机字符串是

“abcdefghij”，那么连接后的结果即字符串“1234567890abcdefghij”）。SMMS 将连接后的字符串使用 hashAlgorithm 定义的哈希算法进行哈希计算，再将其结果进行 base64 编码，得到参数 pwdHash 值即为 SMMS 的认证信息。

b) ISMS 采用同样的方法产生 pwdHash 值, 将其与收到的值进行比较, 如果一致, 则 ISMS 对 SMMS 的认证通过。

指令文件处理过程如下。

a) SMMS 对原始指令 XML 文件使用参数 compressionFormat 指定的压缩格式进行压缩; 对压缩的信息串接消息认证密钥后使用参数 hashAlgorithm 指定的哈希算法计算哈希值, 并对哈希值进行 base64 编码运算形成 commandHash; 对压缩后的信息使用参数 encryptAlgorithm 指定的加密算法加密, 并对加密结果进行 base64 编码运算形成 command。

b) ISMS 收到指令文件后, 首先对 command 进行 base64 反解码, 然后采用参数 encryptAlgorithm 指定的加密算法对解码后的数据进行解密处理, 得到 data; 针对 data 串接消息认证密钥后, 使用 hashAlgorithm 指定的哈希算法计算哈希值, 将得到的哈希值与收到的 commandHash 进行比较, 如果一致, 则对指令文件的完整性校验通过。进一步按照 compressionFormat 指定的压缩格式对 data 进行解压后即得到指令信息。

8.1.5 方法返回值

该方法返回一个 XML 数据流, 数据格式详见 11.13 节, 其描述了本次操作的结果代码、结果描述等信息。

8.2 idc\_commandack()方法

8.2.1 方法原型

public String idc\_commandack (String idcId, String randVal, String pwdHash , String result, String resultHash, Int encryptAlgorithm, Int hashAlgorithm, Int compressionFormat)。

8.2.2 服务请求地址

http://SMMS 服务器 IP 地址/IDCWebService/commandack?wsdl。

8.2.3 参数描述

本方法共使用 9 个参数, 各项参数的描述如表 4 所示。

表 4 idc\_commandack ()方法参数说明

参数名称	参数类型	参数描述
idcId	字符串	IDC/ISP经营者ID, 采用电信管理部门颁发的IDC/ISP许可证号
randVal	字符串	ISMS调用该方法时生成的随机字符串, 长度上限是20
pwdHash	字符串	将用户口令和随机字符串连接后使用hashAlgorithm指定的哈希算法进行哈希运算, 然后进行base64编码得到的结果。 用户口令由设备所在SMMS维护管理, 长度至少为6位, 最多32位
result	字符串	对指令执行结果(见11.11节)使用compressionFormat指定的压缩算法进行压缩, 再对压缩后的信息按照encryptAlgorithm参数的要求进行加密, 然后进行base64编码运算得到的结果, 包括基础数据管理指令、信息安全管理指令和代码表发布指令的执行结果
resultHash	字符串	对指令指令结果使用compressionFormat指定的压缩算法进行压缩, 压缩后串接消息认证密钥, 然后使用hashAlgorithm指定的哈希算法进行哈希运算得到哈希值, 并对哈希值进行base64编码运算形成commandHash, 用于验证完整性。 消息认证密钥由SMMS与ISMS事先配置确定, 长度至少为20位, 最多32位

encryptAlgorithm	整型	对称加密算法如下。 0: 不进行加密，明文传输； 1: AES加密算法； 加密密钥由SMMS与ISMS事先配置确定，长度至少为20字节，最多32字节。 ISMS应根据SMMS的要求完成加密算法的具体实现。ISMS至少应支持采用CBC模式、PKCS7Padding补码方式实现AES加密算法，并可根据SMMS的要求设置AES密钥长度、加密偏移量等参数。
hashAlgorithm	整型	哈希算法如下。 0: 无hash； 1: MD5； 2: SHA-1； ISMS应根据SMMS的要求完成哈希算法的具体实现
compressionFormat	整型	压缩格式如下。 0: 无压缩； 1: Zip压缩格式； ISMS应根据SMMS的要求完成压缩算法的具体实现
commandVersion	字符串	接口方法版本。符合本文件所规定要求的ISMI接口方法为“v2.0”，长度4字节

#### 8.2.4 方法描述

ISMS 接收到 SMMS 下发的信息安全管理指令或代码表发布指令，并将所有指令执行完成后，需要调用本方法，将已执行的指令结果信息发送给 SMMS，同时完成认证和对指令文件的压缩加密处理功能。ISMS 指令文件认证和处理过程中哈希计算结果应采用十六进制字符串（英文字母小写）形式。

认证过程如下。

a) ISMS 产生长度上限为 20 的随机字符串（字符串由数字和大、小写字母构成），将该字符串与 ISMS 中配置的用户口令进行连接（例如，口令是字符串“1234567890”，生成的随机字符串是“abcdefghij”，那么连接后的结果是字符串“1234567890abcdefghij”）。ISMS 将连接后的字符串使用 hashAlgorithm 定义的哈希算法进行哈希计算，再将其结果进行 base64 编码，得到参数 pwdHash 值即为 ISMS 的认证信息。

b) SMMS 采用同样的方法产生 pwdHash 值，将其与收到的进行比较，如果一致，则 SMMS 对 ISMS 的认证通过。

执行结果文件的处理过程如下。

a) ISMS 对执行结果 XML 文件使用参数 compressionFormat 指定的压缩格式进行压缩；对压缩的信息串接消息认证密钥后使用参数 hashAlgorithm 指定的哈希算法计算哈希值，并对哈希值进行 base64 编码运算形成 resultHash；对压缩后的信息使用参数 encryptAlgorithm 指定的加密算法加密，并对加密结果进行 base64 编码运算形成 result。

b) SMMS 收到执行结果文件后，首先对 result 进行 base64 反解码，然后采用参数 encryptAlgorithm 指定的加密算法对解码后的数据进行解密处理，得到 data；针对 data 串接消息认证密钥后，使用 hashAlgorithm 指定的哈希算法计算哈希值，将得到的哈希值与收到的 resultHash 值进行比较，如果一致，则对指令文件的完整性校验通过。进一步按照 compressionFormat 指定的压缩格式对 data 进行解压后即得到执行结果。

#### 8.2.5 返回值



该方法返回一个 XML 数据流，数据格式详见 11.13 节，其描述了本次操作的结果代码、结果描述等信息。

8.3 file\_load 方法

8.3.1 参数描述

file\_load 方法采用 xml 格式上报数据，对原始的上报数据进行加密封装，封装的格式及参数定义见表 5，各节点的格式应符合 11.1 节的要求，具体格式另见 xsd 示例文件。

表 5 数据上报的加密封装格式（节点：fileLoad）

编号	节点	节点名称	必填	数据类型	最大长度	描述
1	idcId	IDC/ISP 经营者 ID	必填	字符串	128	电信管理部门颁发的 IDC/ISP 许可证号
2	dataUpload	数据上报内容	必填	字符串	/	使用参数 compressionFormat 指定的压缩格式对需要上报的数据进行压缩；对压缩后的信息使用参数 encryptAlgorithm 指定的加密算法加密，并对加密结果进行 base64 编码运算后得到的结果。上报的数据包括基础数据、基础数据监测数据、访问日志查询结果、监测日志、过滤日志、信息安全管理指令查询结果以及 ISMS 活动状态等（数据内容见第 11 章）。压缩前的上报数据应符合 11 章相应的数据上报内容要求，且小于 12M
3	encryptAlgorithm	对称加密算法	必填	整型	/	对称加密算法如下。 0：不进行加密，明文传输； 1：AES加密算法。 加密密钥由SMMS与ISMS事先配置确定，长度至少为20字节，最多32字节。 ISMS应根据SMMS的要求完成加密算法的具体实现。ISMS至少应支持采用CBC模式、PKCS7Padding补码方式实现AES加密算法，并可根据SMMS的要求设置AES密钥长度、加密偏移量等参数。
4	compressionFormat	压缩格式	必填	整型	/	压缩格式如下。 0：无压缩； 1：Zip压缩格式。 ISMS应根据SMMS的要求完成压缩算法的具体实现
5	hashAlgorithm	哈希算法	必填	整型	/	哈希算法如下。 0：无hash； 1：MD5； 2：SHA-1。 ISMS应根据SMMS的要求完成哈希算法的具体实现
6	dataHash	数据的哈希结果	选填	字符串	64	将上报的数据按照compressionFormat要求进行压缩后串接消息认证密钥，再根据hashAlgorithm参数进行哈希运算，并进行

						base64编码后的数据结果。 消息认证密钥由SMMS和ISMS通过配置 确定，长度至少为20位，最多32位
7	commandVersion	接口方法版本	必填	字符串	4	符合本文件所规定要求的ISMI接口方法 为“v2.0”

### 8.3.2 方法描述

file\_load 方法可以同时完成对数据文件的消息认证和对数据文件的压缩加密处理功能。ISMS 指令文件认证和处理过程中哈希计算结果应采用十六进制字符串（英文字母小写）形式。

消息认证过程如下。

ISMS 根据 compressionFormat 对上报的数据内容进行压缩，将压缩后的数据串接消息认证密钥后，使用 hashAlgorithm 定义的哈希算法进行哈希计算，并对结果进行 base64 编码，得到参数 dataHash 值即为本次上报数据的消息认证码。

SMMS 端完成对 dataUpload 的 base64 解码和解密后串接消息认证密钥，采用 hashAlgorithm 指定的算法计算出哈希值，将其与 dataHash 进行 base64 解码后的数据进行比较，如果一致，则对 ISMS 本次上报的数据认证通过，本次数据完整有效。

对数据文件处理过程如下。

- a) ISMS 对数据 XML 文件使用参数 compressionFormat 指定的压缩格式进行压缩；对压缩后的信息使用参数 encryptAlgorithm 指定的加密算法加密，并对加密结果进行 base64 编码运算形成 dataUpload。
- b) SMMS 端收到数据文件后，首先进行 base64 解码，然后采用参数 encryptAlgorithm 指定的加密算法进行解密处理，对解密后的信息按照 compressionFormat 指定的压缩格式进行解压后即得到上传数据。

## 9 编码说明

### 9.1 互联网 IP 地址编码

对于 IPv4 的地址，使用点分十进制表示法，字符串最大长度为 15 字节，例如地址 10.2.0.100。

对于 IPv6 的地址，使用冒号分开的十六进制表示法，字符串最大长度为 39 字节，如 2CDA:12:3FC0:567A:8ADE:130:10:94BF。

### 9.2 ICP 备案号

非经营性 ICP 备案号编码格式为：<省/直辖市/自治区的简称>ICP 备<两位数字表示的年份（不足两位在前面补“0”）><六位数字表示的备案序号（不足六位在前面补“0”）>号。

经营性 ICP 备案号编码格式为：<省/直辖市/自治区的简称>ICP 证<主管部门签发的经营许可证号码>号。

## 10 数据代码表

### 10.1 接入方式代码表

接入方式代码见表 6。

表 6 接入方式代码

代 码	接入方式
0	专线
1	虚拟主机
2	主机托管

3	整机租用
999	其他

#### 10.2 单位属性代码表

单位属性代码见表 7。

表 7 单位属性代码

代 码	单位属性名称
1	军队
2	政府机关
3	事业单位
4	企业
5	个人
6	社会团体
999	其他

#### 10.3 证件类型代码表

证件类型代码见表 8。

表 8 证件类型代码

代 码	证件类型
1	工商营业执照号码
2	身份证
3	组织机构代码证书
4	事业法人证书
5	军队代号
6	社团法人证书
7	护照
8	军官证
9	台胞证
999	其他

#### 10.4 机房性质代码表

机房性质代码见表 9。

表 9 机房性质代码

代码号	机房性质
1	租用
2	自建
999	其他

#### 10.5 代理类型代码表

代理类型代码见表 10。

表 10 代理类型代码

代码号	代理类型名称
1	HTTP代理
2	FTP代理
3	Telnet代理
4	SOCKS代理
5	网页代理

6	SSL代理
7	POP3代理
8	TUNNEL代理
9	文献代理
10	SSSO代理
11	ISA代理
12	透传代理
999	其他

#### 10.6 服务内容代码表

服务内容代码见表 11。

表 11 服务内容代码

类型序号	服务内容名称	文 类
500	基础应用	/
501	网络媒体	/
502	电子政务、电子商务	/
503	数字娱乐	/
504	其他	/
1	即时通信	500
2	搜索引擎	500
3	综合门户	500
4	网上邮局	500
5	网络新闻	501
6	博客/个人空间	501
7	网络广告/信息	501
8	单位门户网站	501
9	网络购物	502
10	网上支付	502
11	网上银行	502
12	网上炒股/股票基金	502
13	网络游戏	503
14	网络音乐	503
15	网络影视	503
16	网络图片	503
17	网络软件/下载	503
18	网上求职	504
19	网上交友/婚介	504
20	网上房产	504
21	网络教育	504
22	网站建设	504
23	WAP	504
24	其他	504

#### 10.7 监测规则及过滤规则代码表

监测规则及过滤规则代码见表 12。

表 12 监测规则及过滤规则代码

代 码	规则名称
1	域名
2	URL
3	关键字 <sup>a</sup>
4	源 IP 地址
5	目的 IP 地址
6	源端口
7	目的端口
8	传输层协议

<sup>a</sup> 关键字规则匹配范围仅限于正文标题及正文本身（含附件），ISMS 可选实现基于关键词的附件标题、附件正文违法信息监测与过滤功能。

## 10.8 违法违规情况表

违法违规情况见表 13。

表 13 违法违规情况

代 码	违法违规情况	备 注
1	未备案	相应网站属未备案
2	违法网站	相应网站属于违法网站
999	其他	其他违法违规类型

## 10.9 登记备案属性代码表

登记备案属性代码见表 14。

表 14 登记备案属性代码

代 码	登记备案属性值
0	无
1	经营性网站（ICP经营许可证号）
2	非经营性网站（备案登记号）
3	SP（备案登记号）
4	BBS（BBS备案号）
999	其他

## 10.10 指令优先级代码表

指令优先级代码见表 15。

表 15 指令优先级代码

代 码													指令类型			
十进制	二进制															
1	0	0	0	0	0	0	0	0	0	0	0	1	SMMS 下发 指令	违法网站 列表	目的IP列表	
16	0	0	0	0	0	0	0	1	0	0	0	0			IP域名列表	
64	0	0	0	0	0	1	0	0	0	0	0	0			域名列表	
513	0	0	1	0	0	0	0	0	0	0	0	1		免过滤网站 列表	目的IP列表	
528	0	0	1	0	0	0	0	1	0	0	0	0			IP域名列表	
576	0	0	1	0	0	1	0	0	0	0	0	0			域名列表	
1025	0	1	0	0	0	0	0	0	0	0	0	1		违法信息过滤 指令	目的IP规则	
1026	0	1	0	0	0	0	0	0	0	0	1	0			目的端口规则	
1028	0	1	0	0	0	0	0	0	0	1	0	0			协议类型	TCP

1032	0	1	0	0	0	0	0	0	1	0	0	0	违法信息监测 指令	规则	UDP
1040	0	1	0	0	0	0	0	1	0	0	0	0		源IP规则	
1056	0	1	0	0	0	0	0	1	0	0	0	0		源端口规则	
1088	0	1	0	0	0	0	1	0	0	0	0	0		域名规则	
1152	0	1	0	0	1	0	0	0	0	0	0	0		URL规则	
1280	0	1	0	1	0	0	0	0	0	0	0	0		关键字规则	
1537	0	1	1	0	0	0	0	0	0	0	0	1		目的IP规则	
1538	0	1	1	0	0	0	0	0	0	0	1	0		目的端口规则	
1540	0	1	1	0	0	0	0	0	0	1	0	0		协议类型	TCP
1544	0	1	1	0	0	0	0	0	1	0	0	0		规则	UDP
1552	0	1	1	0	0	0	0	1	0	0	0	0		源IP规则	
1568	0	1	1	0	0	0	1	0	0	0	0	0		源端口规则	
1600	0	1	1	0	0	1	0	0	0	0	0	0		域名规则	
1664	0	1	1	0	1	0	0	0	0	0	0	0		URL规则	
1792	0	1	1	1	0	0	0	0	0	0	0	0		关键字规则	
2048	1	0	0	0	0	0	0	0	0	0	0	0		ISMS下发指令	
备注：1）主要用于标记ISMS执行指令的优先级，当不同指令内容存在冲突（如，违法网站列表记录与免过滤网站列表记录、免过滤网站列表记录与违法信息过滤规则等）优先执行代码数值较小的指令，并按优先级归集有关记录；2）范围1至1024的代码，除列出的以外均为保留；3）对于携带包含2个（或2个以上）特定IP、端口、协议、域名、URL、关键字规则等组合条件的违法信息监测/过滤指令，其优先级按相应单一规则指令优先级的二进制低9位逐位进行或计算，指令优先级范围为1025至2047；4）ISMS侧下发的本地指令优先级范围为2048至4095，由ISMS自行定义和扩展。															

11 数据交换内容描述

11.1 数据格式及匹配要求

所有指令文件、上报记录、消息的数据内容均采用 UTF-8 编码格式。

没有数据类型说明的数据节点/子节点均为字符串类型，其长度属性表示最大长度，实际数据不足最大长度的不应进行补位处理。各节点/子节点长度单位为字节。

所有 timeStamp 节点描述的时间均采用 yyyy-MM-dd HH:mm:ss 格式。

符合本文件所规定要求的 ISMI 接口指令文件、上报记录、消息等均标记为第二版，即“version”节点（名称为“版本标记”，类型为字符串，长度 4 字节）内容均为“v2.0”。

SMMS 和 ISMS 对数据内容采用精确匹配的方式进行校验。各类消息格式另见 xsd 示例文件。

11.2 基础数据查询指令内容

指令的内容如表 16 所示。

表 16 基础数据查询指令数据格式（节点：idcInfoManage）

编号	节点	节点名称	必填	子节点	子节点名称	数据类型	长度	描述
1	commandId	指令 ID	必填			长整型	4	基础数据管理指令唯一 ID，该 ID 由 SMMS 产生
2	type	指令类型	必填			整型	/	0——查询基础数据记录； 1——保留； 2——保留； 3——查询基础数据监测异常
3	commandInfo	指令信息	选填	queryMonitor DayFrom	查询的监测 数据 起始日期	字符串	10	仅在查询监测数据时有效，采用 yyyy-MM-dd 格式 指令类型为 3 时，该节点必填。

			选填	queryMonitor DayTo	查询的监测 数据 结束日期	字符串	10	仅在查询监测数据时有效，采用 yyyy-MM-dd 格式，上报的监测数据应含结束日期当天的数据。 指令类型为 3 时，该节点必填。
			选填	idcId	IDC/ISP 经营 者 ID	字符串	128	IDC 经营单位
			选填	id	客户 ID	长整型	/	(可重复多次) 此项内容为空时，表示该指令对经营者下所有用户生效。
			选填	houseId	机房 ID	长整型	/	(可重复多次) 此项内容为空时，表示该指令对经营者下所有机房生效。
4	timestamp	生成时间	必填			字符串	19	生成该指令的时间

### 11.3 基础数据上报内容

IDC/ISP 基础数据上报内容包括 IDC/ISP 经营者信息、机房基础数据和用户基础数据，数据上报不仅发生在 SMMS 下发基础数据查询指令时，还应在基础数据更新后经 ISMS 核实无误后立刻上传至 SMMS。基础数据上报类型分为两类：ISMS 主动上报，SMMS 查询上报。ISMS 主动上报类型分为：新增、变更、删除三种方式。IDC/ISP 基础数据上报格式如表 17 所示。

表 17 基础数据上报数据格式（节点：basicInfo）

编号	节点	节点名称	必填	长度	描述
1	newInfo	新增的信息	选填	/	需要新增的信息描述，格式见表 18
2	updateInfo	更新的信息	选填	/	需要更新的信息描述，格式见表 19
3	deleteInfo	删除的信息	选填	/	需要删除的信息描述，格式见表 20
4	queryResult	基础数据查询的上报信息	选填	/	见表 24
5	timeStamp	上报时间	必填	19	上报数据的时间

备注：上报信息时只能选择 1-4 中的一个节点信息进行上报

表 18 新增的信息（节点：newInfo）

编号	节点	节点名称	必填	长度	数据类型	描述
1	idcId	IDC/ISP 经营者 ID	必填	128	字符串	电信管理部门颁发的 IDC/ISP 许可证号
2	idcName	IDC/ISP 经营者名称	选填	128	字符串	经营者名称，与许可证上名称一致 <sup>a</sup>
3	idcAdd	IDC/ISP 经营者地址	选填	128	字符串	经营者通信地址 <sup>a</sup>
4	idcZip	邮编	选填	6	字符串	对应经营者通信地址的邮编 <sup>a</sup>
5	corp	企业法人	选填	128	字符串	企业法人 <sup>a</sup>
6	idcOfficer	网络信息安全责任人信息	选填	/		单位的网络安全责任人信息与联系方式，具体信息见表 26 <sup>a</sup>
7	emergencyContact	应急联系人信息	选填	/		单位应急联系人信息与联系方式，具体信息见表 26 <sup>a</sup>
8	houseCount	IDC 业务机房/ISP 业务节点数量	选填	长整形		新增机房数量
9	houseInfo	IDC 业务机房/ISP 业务节点数据	选填	/		新增机房数据，每个机房对应一个记录，记录的具体数据内容见表 25 (可重复多次) 新增机房数据时必填

10	userInfo	用户数据	选填	/		新增用户数据，每个用户对应一个记录，记录的具体内容见表 27（可重复多次） 新增用户数据时必填
----	----------	------	----	---	--	--

<sup>a</sup> 仅在新增时为必填

表 19 更新的信息（节点：updateInfo）

编号	节点	节点名称	必填	长度	数据类型	描述
1	idcId	IDC/ISP 经营者 ID	必填	128	字符串	电信管理部门颁发的 IDC/ISP 许可证号
2	idcName	IDC/ISP 经营者名称	选填	128	字符串	经营者名称，与许可证上名称一致 <sup>a</sup>
3	idcAdd	IDC/ISP 经营者地址	选填	128	字符串	经营者通信地址 <sup>a</sup>
4	idcZip	邮编	选填	6	字符串	对应经营者通信地址的邮编 <sup>a</sup>
5	corp	企业法人	选填	128	字符串	企业法人 <sup>a</sup>
6	idcOfficer	网络信息安全责任人信息	选填	/	字符串	单位的网络安全责任人信息与联系方式，具体信息见表 26 <sup>a</sup>
7	emergencyContact	应急联系人信息	选填	/	字符串	单位应急联系人信息与联系方式，具体信息见表 26 <sup>a</sup>
8	updateData	更新数据	选填	/		根据下级菜单对相应数据进行更新，新增机房信息或更新机房相关数据参照表 25，新增用户信息或更新用户相关数据见表 27（仅提交变更数据项） <sup>a</sup>

<sup>a</sup> 该信息如需更新才填写对应内容

表 20 删除的信息（节点：deleteInfo）

编号	节点	节点名称	必填	长度	数据类型	描述
1	idcId	IDC/ISP 经营者 ID	必填	128	字符串	电信管理部门颁发的 IDC/ISP 许可证号
2	deleteData	删除数据	选填	/		指定删除数据的 ID，见表 21

备注：如果不填写删除数据，则删除 IDC/ISP 经营者的全部基础数据信息

表 21 删除数据（节点：deleteData）

编号	节点	节点名称	必填	长度	描述
1	house	删除的机房数据	选填	/	删除的机房数据，具体数据见表 22（可重复多次）
2	user	删除的用户数据	选填	/	删除的用户数据，具体数据见表 23（可重复多次）

备注：1、2 上报时至少填报一项，如果删除机房，则 SMMS 系统将该机房下对应的用户信息一起删除

表 22 删除的机房数据（节点：house）

编号	节点	节点名称	必填	长度	数据类型	描述
1	houseId	机房 ID	必填	/	长整型	删除的机房 ID 或者要从中删除互联网出入口/IP 地址段的机房 ID
2	gatewayId	链路 ID	选填	/	长整型	删除的机房链路 ID
3	ipSegId	IP 段 ID	选填	/	长整型	删除的机房 IP 段 ID

表 23 删除的用户数据（节点：user）

编号	节点	节点名称	子节点	子节点名称	必填	数据类型	长度	描述
----	----	------	-----	-------	----	------	----	----



1	userId	用户 ID	/	/	必填	长整型	32	删除的用户 ID 或者要从中删除应用服务/应用服务域名/占用机房信息的用户 ID
2	service	删除的应用服务数据 <sup>a</sup>	serviceId	应用服务 ID	必填	长整型	/	删除的应用服务 ID 或者要从中删除应用服务域名及占用机房信息的应用服务 ID
			domainId	应用服务的域名 ID	选填	长整型	/	删除的应用服务域名 ID (应用服务 ID 必填) (可重复多次)
			hhId	占用机房信息 ID	选填	长整型	/	删除应用服务的占用机房信息 ID (应用服务 ID 必填) (可重复多次)
3	hhId	占用机房信息 ID	/	/	选填	长整型	/	删除其他用户的占用机房信息 ID

<sup>a</sup> 该节点选填

表 24 基础数据查询的上报信息 (节点: queryResult)

编号	节点	节点名称	必填	数据类型	长度	数据类型	描述
1	commandId	指令 ID	必填	长整型	4	长整型	对应的查询指令 ID
2	idcId	IDC/ISP 经营者 ID	必填	字符串	128	字符串	电信管理部门颁发的 IDC/ISP 许可证号
3	idcName	IDC/ISP 经营者名称	必填	字符串	128	字符串	经营者名称, 与许可证上名称一致
4	idcAdd	IDC/ISP 经营者地址	必填	字符串	128	字符串	经营者通信地址
5	idcZip	邮编	必填	字符串	6	字符串	对应经营者通信地址的邮编
6	corp	企业法人	必填	字符串	128	字符串	企业法人
7	idcOfficer	网络信息安全责任人信息	必填	/	/	字符串	单位的网络安全责任人信息与联系方式, 具体信息见表 26
8	emergencyContact	应急联系人信息	必填	/	/	字符串	单位应急联系人信息与联系方式, 具体信息见表 26
9	houseInfo	机房数据	必填	/	/		机房数据, 每个机房对应一个记录, 记录的具体数据内容见表 25 (可重复多次)
10	userInfo	用户数据	必填	/	/		IDC 用户数据, 每个用户对应一个记录, 记录的具体内容见表 27 (可重复多次)

表 25 机房数据 (节点: houseInfo)

编号	节点	节点名称	子节点	子节点名称	必填	数据类型	长度	描述
1	houseId	机房 ID	/	/	必填	长整型	32	当前机房的编号, 由 IDC 或 ISP 经营者产生, 在本单位中惟一
2	houseName	机房名称	/	/	必填	字符串	128	机房的名称
3	houseType	机房性质	/	/	必填	整型	/	机房性质, 见 10.4 节
4	houseProvince	机房所在省	/	/	必填	长整型	6	机房所在省或直辖市的行政区

		或直辖市						划数字代码, 见 GB/T 2260-2007
5	houseCity	机房所在市或区(县)	/	/	必填	长整型	6	机房所在市或区(县)的行政区划数字代码, 见 GB/T 2260-2007
6	houseCounty	机房所在县	/	/	选填	长整型	6	机房所在县的行政区划数字代码, 见 GB/T 2260-2007
7	houseAdd	机房地址	/	/	必填	字符串	128	IDC/ISP 机房的通信地址
8	houseZip	邮编	/	/	必填	字符串	6	对应机房通信地址的邮编
9	houseOfficer	机房网络信息安全责任人信息	/	/	必填	/	/	机房负责人信息与联系方式, 具体信息见表 26
10	gatewayInfo	链路信息 <sup>a</sup>	id	链路信息 ID	必填	长整型	/	机房互联网出入口(含专线)ID, 由 ISMS 定义, 当前机房中惟一
			bandWidth	链路带宽	必填	长整型	/	机房互联网出入口带宽(单位: Mbit/s)
			linkType	链路类型	必填	整型		机房互联网出入口类型: 1, 电信; 2, 联通; 3, 移动; 4, 铁通; 9, 其他
			accessUnit	链路接入单位信息	必填	字符串		接入单位指为 ISMS 覆盖的业务链路的上联单位(为 IDC/ISP 经营者提供接入的接入单位)
			gatewayIp	网关 IP 地址	必填	字符串	64	机房互联网出入口网关 IP 地址
11	ipSegInfo	IP 地址段信息 <sup>a</sup>	id	IP 地址段序号	必填	长整型	/	IP 地址段资源的编号, 由 ISMS 定义, 当前机房中惟一
			startIp	起始 IP 地址	必填	字符串	64	该地址段的起始 IP 地址
			endIp	终止 IP 地址	必填	字符串	64	该地址段的终止 IP 地址, 当起始 IP 地址与终止 IP 地址相同时, 表示该地址段只有一个地址
			type	IP 地址使用方式	必填	整型	/	IP 地址使用方式, 包括: 0——静态; 1——动态; 2——保留; <u>3——专线</u>
			user	使用人或者单位	选填	字符串	128	使用该 IP 段的单位名称, 如果是个人需要填写姓名
			idType	使用人的证件类型	选填	整型	/	使用人的证件类型, 见 10.3 节
			idNumber	对应证件号码	选填	字符串	32	对应的使用人的证件号码
			sourceUnit	来源单位	必填	字符串	128	特定单个 IP/IP 段的来源, 自有的填写自己的单位名称, 用户携带的填写用户单位名称
			allocationUnit	分配单位	必填	字符串	128	IDC/ISP 经营者所持有 IP 的上级分配单位: 集团/省公司/市公司分配的写集团/省/市公司名称, 自己申请的写 ICANN、

批注 [钱康1]: 添加专线标识, 企业填报“3”时为专线数据

								APNIC 或其他地址分配单位的名称
			useTime	分配使用时间	必填	字符串	10	该 IP 段分配给使用人的时间或使用方式转变的时间，采用 yyyy-MM-dd 格式
12	frameInfo	机架信息 <sup>a</sup>	id	机架信息 ID	必填	长整型	/	机架信息的编码，由 ISMS 定义，当前机房中唯一
			useType	使用类型	必填	整型	/	1-自用 2-出租
			distribution	分配状态	必填	整型	/	1-未分配 2-已分配
			occupancy	占用状态	必填	整型	/	1-未占用 2-已占用
			frameName	机架/机位名称	必填	字符串	128	

<sup>a</sup> 该节点必填，可重复多次

批注 [钱康2]: 报送专线资源时，该节点所有子节点全部填“0”

表 26 人员信息

编号	节点	节点名称	必填	数据类型	长度	描述
1	name	姓名	必填	字符串	32	人员姓名
2	idType	证件类型	必填	整型	/	人员的证件类型，见 10.3 节，有效类型只有身份证、护照、军官证、台胞证
3	id	证件号码	必填	字符串	32	对应的证件号码
4	tel	固定电话	必填	字符串	32	固定电话
5	mobile	移动电话	必填	字符串	32	移动电话
6	email	email 地址	必填	字符串	64	email 地址

表 27 用户信息（节点：userInfo）

编号	节点	节点名称	必填	数据类型	长度	描述
1	id	用户 ID	必填	长整型	/	用户唯一 ID，由 IDC/ISP 经营者产生，在本单位中唯一
2	nature	用户属性	必填	整型	/	1) 提供互联网应用服务的用户； 2) 其他用户
3	info	用户信息	必填	/	/	提供互联网应用服务的用户信息见表 28；其他用户见表 31

备注：用户属性不能直接变更，需先删除原有用户属性信息，再新增另一种用户属性信息，上报用户信息时需要上报用户占用的所有机房信息。

表 28 提供互联网应用服务的用户信息（节点：info）

编号	节点	节点名称	必填	数据类型	长度	描述
1	unitName	单位名称	必填	字符串	128	单位名称（个人填写个人姓名）
2	unitNature	单位属性	必填	整型	/	单位属性，见 10.2 节
3	idType	证件类型	必填	整型	/	单位证件类型，见 10.3 节
4	idNumber	证件号码	必填	字符串	32	对应的证件号码
5	officer	网络信息安全责任人信息	必填	/	/	网络信息安全责任人信息，具体见表 26
6	add	单位地址	必填	字符串	128	单位地址
7	zipCode	邮政编码	必填	字符串	6	邮政编码
8	serviceInfo	服务信息	必填	/	/	服务信息，见表 29 (可重复多次)

9	registerTime	注册时间	必填	字符串	10	用户的注册时间，采用 yyyy-MM-dd 格式
---	--------------	------	----	-----	----	--------------------------

表 29 服务信息（节点：serviceInfo）

编号	节点	节点名称	子节点	子节点名称	必填	数据类型	长度	描述
1	serviceId	服务 ID	/	/	必填	长整型	/	服务编号，该用户内惟一
2	serviceContent	服务内容	/	/	必填	整型	/	填写服务的内容，见 10.6 节（可重复多次）
3	regType	备案类型	/	/	选填	整型	/	网站登记备案类型，见 10.9 节
4	regId	备案号或许可证号	/	/	选填	字符串	64	网站备案号或许可证号
5	setMode	接入方式	/	/	必填	整型	/	接入方式，见 10.1 节
6	business	业务类型			必填	整型		1-IDC 业务 2-ISP 业务
7	domain	域名信息 <sup>a</sup>	id	域名 ID	必填	长整型	/	域名的 ID，该应用服务内惟一
			name	域名	必填	字符串	128	对应该域名 ID 的域名
8	housesHoldInfo	占用机房信息 <sup>b</sup>	hhId	占用机房信息 ID	必填	长整型	/	占用机房信息的 ID，由 IDC/ISP 经营者产生，当前应用服务惟一
			houseId	IDC/ISP 机房 ID	必填	长整型	/	占用机房 ID，由 IDC/ISP 经营者产生，在本单位中惟一
			distributeTime	资源分配时间	必填	字符串	10	资源分配时间的时间，采用 yyyy-MM-dd 的格式
			virtualServer	虚拟主机信息	选填			含有虚拟主机信息时必填，见表 29（续）
			frameInfolId	机架 ID	选填	长整型		机架编号 ID，当 IDC 业务时必填，ISP 业务时选填
			bandWidth	网络带宽	选填	长整型	/	网络带宽（单位：Mbit/s）
			ipTrans	IP 地址转换信息	必填	/	/	在该机房中所分配的 IP 地址段信息，内容见表 30，有地址转换的需要填写对应的私网地址（可重复多次）
<sup>a</sup> 该节点选填，可重复多次。								
<sup>b</sup> 该节点必填，可重复多次。								

批注 [钱康3]: 专线数据在此填写“0”

表 29 （续）虚拟主机信息

编号	节点	节点名称	必填	数据类型	长度	描述
1	virtualhostName	虚拟主机名称	必填	字符串	128	
2	virtualhostState	虚拟主机状态	选填	整型		
3	virtualhostType	虚拟主机类型	必填	整型		共享式/专用式/云虚拟
4	virtualhostAddress	虚拟主机网络地址	必填	字符串		
5	virtualhost	虚拟主机管理地址	必填	字符串		

	ManagementAddress					
--	-------------------	--	--	--	--	--

表 30 IP 地址转换信息（节点：ipTrans）

编号	节点	节点名称	子节点	子节点名称	必填	长度	描述
1	internetIp	互联网 IP 地址段	startIp	互联网起始 IP 地址	必填	64	该地址段的互联网起始 IP 地址
			endIp	互联网终止 IP 地址	必填	64	该地址段的互联网终止 IP 地址，当起始 IP 地址与终止 IP 地址相同时，表示该地址段只有一个地址
2	netIp	对应私网 IP 地址段 <sup>a</sup>	startIp	对应的私网起始 IP 地址	选填	64	对应的私网起始 IP 地址
			endIp	对应的私网终止 IP 地址	选填	64	对应的私网终止 IP 地址，当起始 IP 地址与终止 IP 地址相同时，表示该地址段只有一个地址

<sup>a</sup> 该节点选填

表 31 其他用户信息（节点：info）

编号	节点	节点名称	子节点	子节点名称	必填	数据类型	长度	描述
1	unitName	单位名称	/	/	必填	字符串	128	单位名称（个人填写个人姓名）
2	unitNature	单位属性	/	/	必填	整型	/	单位属性，见 10.2 节
3	idType	证件类型	/	/	必填	整型	/	单位证件类型，见 10.3 节
4	idNumber	证件号码	/	/	必填	字符串	32	对应的证件号码
5	officer	网络信息安全责任人信息	/	/	必填	/	/	网络信息安全负责人信息 具体见表 26
6	add	单位地址	/	/	必填	字符串	128	单位地址
7	zipCode	邮政编码	/	/	必填	字符串	6	邮政编码
8	serviceRegTime	服务开通时间	/	/	必填	字符串	10	用户的服务开通时间，采用 yyyy-MM-dd 格式
9	houseHoldInfo	占用机房信息 <sup>a</sup>	hhId	占用机房信息 ID	必填	长整型	/	占用机房信息的 ID，由 IDC/ISP 经营者产生，在本单位中惟一
			houseId	IDC/ISP 机房 ID	必填	长整型	/	占用机房 ID，由 IDC/ISP 经营者产生，在本单位中惟一
			distributeTime	资源分配时间	必填	字符串	10	资源分配时间的时间，采用 yyyy-MM-dd 的格式
			ipSeg	IP 地址信息	必填	/	/	在该机房中所分配的 IP 地址段信息，内容见表 32（可重复多次）
			bandWidth	网络带宽	选填	长整型	/	网络带宽（单位：Mbit/s）
10	registerTime	注册时间	/	/	必填	字符串	10	用户的注册时间，采用 yyyy-MM-dd 格式

<sup>a</sup> 该节点必填，可重复多次

表 32 IP 地址段（节点：ipSeg）

编号	节点	节点名称	必填	数据类型	长度	描述
1	ipId	IP 段编号	必填	长整型	/	IP 段编号 ID，由 IDC/ISP 经营者产生，在本单位中惟一
	startIp	起始 IP 地址	必填	字符串	64	该地址段的起始 IP 地址+（专线）
	endIp	终止 IP 地址	必填	字符串	64	该地址段的终止 IP 地址+（专线），当起始 IP 地址与终止 IP 地址相同时，表示该地址段只有一个地址

**批注 [钱康4]:** 对于专线资源上报的活跃域名，需要在此字段添加（专线）标识  
例：192.168.1.1(专线)

#### 11.4 基础数据监测数据上报内容

IDC/ISP 基础数据监测数据包括对应 IP、域名等信息以及违法违规信息、IP 使用信息等，IDC/ISP 基础数据监测数据格式如表 33 所示。

表 33 基础数据监测数据上报数据格式(节点: idcMonitor)

编号	节点	节点名称	必填	数据类型	长度	描述
1	commandId	指令 ID	选填	长整型	4	对应的查询指令 ID，仅在查询上报时有效
2	idcId	IDC/ISP 经营者 ID	必填	字符串	18	电信管理部门颁发的 IDC/ISP 许可证号
3	houseMonitor <sup>a</sup>	机房监测数据	选填	/	/	每个机房一个记录（可重复多次）
4	timeStamp	生成时间	必填	字符串	19	生成上报数据的时间

<sup>a</sup>: 如果部分(或全部)机房没有监测到基础数据异常，该节点内容包括机房 ID“Id”子节点(长整型)和零报告记录“reportNA”子节点(字符串型，内容为“NA”)，每个机房一个记录。

**批注 [钱康5]:** 对于专线资源上报的活跃域名，需要在此字段添加（专线）标识  
例：192.168.1.1(专线)

表 34 机房监测数据(节点: houseMonitor)

编号	节点	节点名称	子节点	子节点名称	必填	数据类型	长度	描述
1	id	机房 ID	/	/	必填	长整型	/	当前机房 ID，由 IDC 或 ISP 经营者产生，在本单位中惟一
2	ip	应用服务 IP	/	/	必填	字符串	64	监测到的应用服务 IP
3	port	端口	/	/	必填	长整型	/	监测到的应用服务端口
4	domain	域名	/	/	选填	字符串	128	监测到的实际域名
5	serviceType	服务内容	/	/	选填	整型	/	对应的服务内容，见 10.6 节 当域名已备案时，服务内容为必填
6	firstFound	首次发现时间	/	/	必填	字符串	19	从打开基础数据监测功能后，首次监测到该异常的时间，采用 yyyy-MM-dd HH:mm:ss 格式
7	lastFound	最近一次发现时间	/	/	必填	字符串	19	当天最后一次发现该异常的时间，采用 yyyy-MM-dd HH:mm:ss 格式
8	visitCount	24 小时累积访问量			必填	长整型		域名访问量按照该域名的访问次数统计 IP 访问量按照访问该 IP 地址的次数统计
9	protocol	传输层协议类型			必填	整型		1- TCP 2- UDP
10	illegalInfo	违法违规信息 <sup>a</sup>	illegalType	违法违规情况	必填	整型	/	违法违规的情况，见 10.8 节
			currentState	当前状态	必填	整型	/	该网站的当前状态： 0——未处置； 1——已处置

			user	用户名	必填	字符串	128	下达处置指令的 ISMS 用户所用用户名，系统自动处置则填写“ISMS”
11	ipInfo	IP 使用信息 <sup>a</sup>	regError	登记异常	必填	整型	/	0——正常； 1——IP 登记保留，实际为启用； 2——IP 登记域名有误； 3——IP 未登记
			regDomain	登记域名	选填	字符串	128	该 IP 登记的域名
<sup>a</sup> 当有监测到的域名时,节点 11 必填								
备注：活跃资源监测数据中如果存在监测到的异常数据，需要填写异常数据相关信息，主动上报给 SMMS。								

11.5 访问日志查询指令内容

SMMS 生成的访问日志查询指令数据内容如表 35 所示。

表 35 访问日志查询指令数据格式（节点：logQuery）

编号	节点	节点名称	子节点	子节点名称	必填	数据类型	长度	描述
1	commandId	日志查询指令 ID			必填	长整型	4	日志查询指令唯一 ID，该 ID 由 SMMS 产生
2	idcId	IDC/ISP 经营者 ID			必填	字符串	128	电信管理部门颁发的 IDC/ISP 许可证号
3	commandInfo	指令信息	houseId	机房 ID	必填	长整型	/	目标机房 ID，由 IDC/ISP 经营者产生，在本单位中惟一
			startTime	起始时间	必填	字符串	19	查询的时间段起始时间，采用 yyyy-MM-dd HH:mm:ss 格式
			endTime	终止时间	可选	字符串	19	查询的时间段终止时间，采用 yyyy-MM-dd HH:mm:ss 格式
			srcIp	源 IP	选填	/	/	查询的源 IP，以 IP 段的形式描述，内容见表 32 的起始 IP 地址和终止 IP 地址子节点。
			destIp	目的 IP	选填	/	/	查询的目的 IP，以 IP 段的形式描述，内容见表 32 的起始 IP 地址和终止 IP 地址子节点。
			srcPort	源端口	选填	长整型	/	查询的源端口
			dstPort	目的端口	选填	长整型	/	查询的目的端口
			protocolType	传输层协议类型	选填	长整型	/	当包含 srcPort 或 dstPort 时为必填。 1——TCP 2——UDP
			url	URL	选填	字符串	2048	经 base64 编码后的待查询 url（精确查询）
4	timeStamp	生成时间			必填	字符串	19	生成该查询指令的时间
备注：endTime 不填写时，endTime 默认为 startTime 加两个小时								

组合条件：a、源 IP 地址+源端口+查询时间
b、源 IP 地址+查询时间
c、目的 IP 地址+目的端口+查询时间
d、用户访问 URL+查询时间
在该四种组合条件中选择其他选项

11.6 访问日志查询结果上报内容

IDC/ISP 企业系统向 SMMS 上报的访问日志查询结果报数据内容如表 36 所示。

表 36 访问日志查询结果上报数据格式(节点: logQueryResult)

编号	节点	节点名称	子节点	子节点名称	必填	数据类型	长度	描述
1	commandId	查询指令 ID	/	/	必填	长整型	4	对应的日志查询指令 ID
2	idcId	IDC/ISP 经营者 ID	/	/	必填	字符串	128	电信管理部门颁发的 IDC/ISP 许可证号
3	result	执行结果 <sup>a</sup>	logAmount	符合查询条件的访问日志总数	必填	长整型	/	该指令的查询结果总数为每次上报文件记录的总数
			endFlag	结束标志	必填	整型	/	查询指令的执行结果标志: 标志指令的执行结果: 0——最后一份符合条件的访问日志,本次上报结束后,上报全部完成; 1——尚未结束上报,还有日志需要上传
			msgInfo	执行结果描述	选填	字符串	128	查询指令的执行结果描述
4	log	日志 <sup>b</sup>	logId	日志记录 ID	必填	长整型	/	日志记录的惟一编码
			houseId	机房 ID	必填	长整型	/	报送结果的机房 ID,由 IDC 或 ISP 经营者产生,在本单位中惟一
			srcIp	源 IP	必填	字符串	64	源 IP 地址
			destIp	目的 IP	必填	字符串	64	目的 IP 地址
			srcPort	源端口	必填	长整型	/	源端口
			destPort	目的端口	必填	长整型	/	目的端口
			url	URL	选填	字符串	2048	采用 base64 编码后的 URL (HTTP 协议需要留存 URL)
5	timeStamp	生成时间						
			accessTime	访问时间	必填	字符串	19	访问时间,采用 yyyy-MM-dd HH:mm:ss 的格式
5	timeStamp	生成时间	/	/	必填	字符串	19	生成该 xml 的时间
<sup>a</sup> 该节点必填。								
<sup>b</sup> 该节点选填,可重复多次								

11.7 违法信息安全管理指令内容

SMMS 生成的违法信息安全管理指令数据内容如表 37 所示。

表 37 违法管理指令格式及描述(节点:command)

编号	节点	节点名称	子节点	子节点名称	必填	数据类型	长度	描述
1	commandId	管理指令 ID	/	/	必填	长整型	4	管理指令的惟一编码,由 SMMS 产生,用于对特定违



								法信息安全管理指令进行修改或撤销。
2	type	管理指令类型	/	/	必填	整型	/	管理指令的类型： 1——监测指令； 2——过滤指令
3	rule	规则 <sup>a</sup>	subtype	规则类型	必填	整型	/	监测规则、过滤规则代码，见10.7节。
			valueStart	规则内容的起始值	必填	字符串	128	规则类型为IP类的情况下是规则内容的起始值，其他类型规则直接是规则内容
			valueEnd	规则内容的结束值	选填	字符串	128	规则内容的结束值，仅在规则类型为IP类的情况下有效
			keywordRange	关键词规则的匹配范围	选填	整型	/	关键词规则的匹配范围： 0——正文标题及正文本身； 1——附件文件题目； 2——附件正文 (可重复多次)
4	action	处置 <sup>b</sup>	reason	过滤原因	必填	字符串	128	仅对过滤规则有效，用于说明过滤的原因。
			log	日志记录	必填	整型		是否对中标的网络数据进行记录： 0——不记录； 1——记录
			report	日志上传	必填	整型		是否对中标的网络数据的日志记录进行上报： 0——不上传； 1——上传
5	time	时间 <sup>b</sup>	effectTime	生效时间	必填	字符串	19	指令的生效时间，采用 yyyy-MM-dd HH:mm:ss 格式
			expiredTime	过期时间	必填	字符串	19	指令的失效时间，采用 yyyy-MM-dd HH:mm:ss 格式
6	range	生效范围 <sup>c</sup>	idcId	IDC 或 ISP 经营者 ID	必填	字符串	128	该指令生效的经营者
			houseId	机房 ID	必填	长整型	/	该指令生效的经营者对应的机房 (可重复多次)
7	privilege	权限 <sup>b</sup>	owner	指令属主	必填	字符串	32	下发指令的 SMMS 用户名
			visible	可读标记	必填	整型	/	该指令是否对 ISMS 可读： 0——不可读； 1——可读
8	operationType	操作类型	/	/	必填	整型	/	对该记录的操作类型，包括： 0——新增； 1——删除
9	level	规则优先级	/	/	必填	字符串	12	见表 10.10 节，二进制代码，多个规则时，规则优先级以最

								高级为准填写
10	timeStamp	生成时间	/	/	必填	字符串	19	生成该 xml 的时间
<sup>a</sup> 该节点必填，可重复多次，因此同一指令可以有多个规则（上限 100 条），各规则之间为逻辑“与”关系。表达“或”的关系需用多条指令来实现。 <sup>b</sup> 该节点必填。 <sup>c</sup> 该节点选填								

### 11.8 违法信息监测记录上报内容

ISMS 向 SMMS 上报的监测记录数据内容如表 38 所示。

表 38 监测记录上报数据格式及描述（节点：monitorResult）

编号	节点	节点名称	子节点	子节点名称	必填	数据类型	长度	描述
1	idcId	IDC/ISP 经营者 ID	/	/	必填	字符串	128	电信管理部门颁发的 IDC/ISP 许可证号
2	log	监测日志 <sup>a</sup>	logId	监测日志记录 ID	必填	长整型	/	监测记录本地 ID
			commandId	监测指令 ID	必填	长整型	/	命中的监测指令 ID
			houseId	机房 ID	必填	长整型	/	报送结果的机房 ID，由 IDC 或 ISP 经营者产生，在本单位中唯一
			srcIp	源 IP	必填	字符串	64	源 IP 地址
			destIp	目的 IP	必填	字符串	64	目的 IP 地址
			srcPort	源端口	必填	长整型	/	源端口
			destPort	目的端口	必填	长整型	/	目的端口
			domain	域名	选填	字符串	128	域名
			view	累积访问量	选填	长整型		累积访问量
			proxyType	代理类型	选填	整型	/	代理类型，见 10.5 节
			proxyIp	代理 IP	选填	字符串	64	代理 IP
			proxyPort	代理端口	选填	长整型	/	代理端口
			title	标题	选填	字符串	128	采用 base64 编码后的标题
			content	内容	选填	字符串	/	采用 base64 编码后的内容，编码之前的文件大小不超过 1M
			url	URL	选填	字符串	2048	采用 base64 编码后的 URL
			attachment	附件	选填	/	/	相关附件，见表 39（可重复多次）
			gatherTime	采集时间	必填	字符串	19	采集时间，采用 yyyy-MM-dd HH:mm:ss 的格式
3	timeStamp	生成时间	/	/	必填	字符串	19	生成该监测日志的时间
<sup>a</sup> 该节点必填，可重复多次								

表 39 附件(节点：attachment)

编号	节点	字段	必填	长度	描述
1	title	附件文件标题	必填	128	附件文件的标题
2	file	附件文件	必填	/	采用 base64 编码后的附件文件，原文件不能超过 10M

### 11.9 违法信息过滤记录上报内容

ISMS 向 SMMS 上报的过滤记录数据内容如表 40 所示。

表 40 过滤记录上报数据格式及描述（节点：filterResult）

编号	节点	节点名称	子节点	子节点名称	必填	数据类型	长度	描述
1	idcId	IDC/ISP 经营者 ID	/	/	必填	字符串	128	电信管理部门颁发的 IDC/ISP 许可证号
2	log	过滤日志 <sup>a</sup>	logId	过滤日志记录 ID	必填	长整型	/	过滤记录本地 ID
			commandId	过滤指令 ID	必填	长整型	/	命中的过滤指令 ID
			houseId	机房 ID	必填	长整型	32	报送结果的机房 ID，由 IDC/ISP 经营者产生，在本单位中惟一
			srcIp	源 IP	必填	字符串	64	源 IP 地址
			destIp	目的 IP	必填	字符串	64	目的 IP 地址
			srcPort	源端口	必填	长整型	/	源端口
			destPort	目的端口	必填	长整型	/	目的端口
			domain	域名	选填	字符串	128	域名
			view	累积访问量	选填	长整型	/	累积访问量
			proxyType	代理类型	选填	整型	/	代理类型，见 10.5 节
			proxyIp	代理 IP	选填	字符串	64	代理 IP
			proxyPort	代理端口	选填	长整型	/	代理端口
			title	标题	选填	字符串	128	采用 base64 编码后的标题
			content	内容	选填	字符串	/	采用 base64 编码后的内容，编码之前的文件大小不超过 1M
			url	URL	选填	字符串	2048	采用 base64 编码后的 URL
			attachment	附件	选填	/	/	相关附件，见表 39（可重复多次）
			gatherTime	采集时间	必填	字符串	19	采用 yyyy-MM-dd HH:mm:ss 的格式
3	timeStamp	生成时间	/	/	必填	字符串	19	生成该过滤日志的时间

<sup>a</sup> 该节点必填，可重复多次

#### 11.10 代码表发布指令内容

SMMS 生成的代码表发布指令数据内容如表 41 所示。

表 41 代码表发布指令文件数据格式描述(节点:codeList)

编号	节点	节点名称	子节点	子节点名称	必填	数据类型	长度	描述
1	commandId	代码表发布 指令序号	/	/	必填	长整型	4	代码表发布指令的惟一编码，由 SMMS 产生
2	jrls	接入方式	jrlsXx	接入方式代码 信息	必填	/	/	接入方式代码信息，子节点数据内容见表 42（子节点可重复多次）
3	dwsx	单位属性	dwsxXx	单位属性代码 信息	必填	/	/	单位属性代码信息，子节点数据内容见表 42（子节点可重复多次）
4	zjlx	证件类型	zjlxXx	证件类型代码 信息	必填	/	/	证件类型代码信息，子节点数据内容见表 42

								(子节点可重复多次)
5	jfxz	机房性质	jfxzXx	机房性质代码信息	必填	/	/	机房性质代码信息, 子节点数据内容见表 42 (子节点可重复多次)
6	dllx	代理类型	dllxXx	代理类型代码信息	必填	/	/	代理类型代码信息, 子节点数据内容见表 42 (子节点可重复多次)
7	fwnr	服务内容	fwnrXx	服务内容代码信息	必填	/	/	服务内容代码信息, 子节点数据内容见表 43 (子节点可重复多次)
8	gzlx	监测规则及过滤规则类型	gzlxXx	监测规则及过滤规则类型代码信息	必填	/	/	监测规则及过滤规则代码信息, 子节点数据内容见表 42 (子节点可重复多次)
9	wfwgqk	违法违规情况	wfwgqkXx	违法违规情况代码信息	必填	/	/	违法违规情况代码信息, 子节点数据内容见表 42 (子节点可重复多次)
10	timeStamp	生成时间	/	/	必填	字符串	19	生成代码表发布内容的时间

表 42 除服务内容外的代码表数据格式

编号	节点	节点名称	必填	数据类型	长度	描述
1	id	ID	必填	整型	/	代码
2	mc	名称	必填	字符串	32	当前代码对应的属性值
3	bz	备注	选填	字符串	64	备注
4	sfyx	是否有效	必填	整型	/	0——无效; 1——有效

表 43 服务内容代码表数据格式 (节点: fwnrXx)

编号	节点	节点名称	必填	数据类型	长度	描述
1	id	ID	必填	整型	/	代码
2	mc	名称	必填	字符串	32	当前代码对应的属性值
3	fl	父类 ID	选填	整型	/	当前属性所属的父类 ID, 已经是父类节点的此处不填
4	bz	备注	选填	字符串	64	备注
5	sfyx	是否有效	必填	整型	/	0——无效; 1——有效

#### 11.11 指令执行情况上报内容

ISMS 生成的指令执行情况上报数据内容如表 44 所示。

表 44 指令执行情况上报文件格式描述 (节点: idcCommandAck)

编号	节点	节点名称	子节点	子节点名称	必填	数据类型	长度	描述
1	idcId	IDC/ISP 经营者 ID	/	/	必填	字符串	128	电信管理部门颁发的 IDC/ISP 许可证号
2	commandAck	执行情况 <sup>a</sup>	houseId	机房 ID	选填	长整型	32	报送结果的机房 ID, 由 IDC/ISP 经营者产生, 在本单位中惟一 如果指令的执行无法明确到机房, 该节点可以选填
			commandId	指令 ID	必填	长整型	/	指令惟一 ID, 该 ID 由

			type	指令类型	必填	整型	/	SMMS 产生 指令惟一 ID，该 ID 由 SMMS 产生，包括： 1——违法信息监测指令； 2——违法信息过滤指令； 3——保留 4——代码发布指令 5——免过滤网站列表指令 6——违法网站列表指令 7——活跃资源访问量查询指令 8——违法信息管理查询指令
			resultCode	执行结果代码	必填	整型		执行结果代码 0——完全成功； 1——保留； 2——失败
			view	访问量	选填	长整型	/	当指令类型为 7 时，该节点必填
			monitorCount	监测指令累积计数	选填	长整型		当指令类型为 8 时，上报执行过的监测指令的累积计数
			filterCount	过滤指令累积计数	选填	长整型		当指令类型为 8 时，上报执行过的过滤指令的累积计数
			msgInfo	执行结果描述	选填	字符串	128	对结果进行描述
3	timeStamp	生成时间	/	/	必填	字符串	19	生成该上报文件的时间

<sup>a</sup> 该节点必填，可重复多次

11.12 ISMS 活动状态上报内容

ISMS 定期向 SMMS 上报活动状态，上报的数据内容如表 45 所示。

表 45 ISMS 活动状态上报内容（节点：activeState）

编号	节点	节点名称	必填	数据类型	长度	描述
1	idcId	IDC/ISP 经营者 ID	必填	字符串	128	电信管理部门颁发的 IDC/ISP 许可证号
2	houseAmount	机房总数	必填	整型	/	机房总数
3	errHouseAmount	异常机房总数	必填	整型	/	出现异常的机房总数
4	errHouseId	异常机房 ID	选填	长整型	32	异常的机房 ID，由 IDC/ISP 经营者产生，在本单位中惟一（可重复多次）
5	timeStamp	上报时间	必填	字符串	19	上报活动状态的时间

11.13 Webservice 方法调用返回文件内容

SMMS 或 ISMS 调用 Webservice 方法后，对端返回的数据内容如表 46 所示。

表 46 Webservice 方法调用返回文件数据格式（节点：return）

编号	节点	字段	必填	数据类型	长度	描述
1	resultCode	错误代码	必填	整型	/	0——处理完成； 1——文件解密失败；

						2——文件校验失败； 3——文件解压缩失败； 4——文件格式异常； 5——文件内容异常； 900——其他异常（存在其他错误， 需重新发送）
2	msg	返回信息	必填	字符串	128	描述错误原因

#### 11.14 基础数据核验处理指令内容

表 47 基础数据核验处理信息（节点：returnInfo）

编号	节点	节点名称	必填	长度	数据类型	描述
1	idcId	IDC/ISP 经营者 ID	必填	128	字符串	电信管理部门颁发的 IDC/ISP 许可证号
2	returnData	退回数据	选填	/		指定退回数据的 ID，见表 48
3	returnCode	退回原因	必填	/	整型	0——上报记录通过核验 1——上报数据与既有数据记录冲突 2——上报数据内容不完整 3——上报数据内容错误 4——其他原因退回
4	returnMsg	退回原因说明	选填	512	字符串	
5	timeStamp	退回时间	必填		字符串	

备注：在对经营单位信息核验处理时，returnData 不填写，在对机房数据或用户数据核验处理时，returnData 必填。

表 48 退回数据（节点：returnData）

编号	节点	节点名称	必填	长度	描述
1	house	退回的机房数据	选填	/	退回的机房数据，具体数据见表 49 （可重复多次）
2	user	退回的用户数据	选填	/	退回的用户数据，具体数据见表 50 （可重复多次）

备注：1、2 退回时须二选一。

表 49 退回的机房数据（节点：house）

编号	节点	节点名称	必填	长度	数据类型	描述
1	houseId	机房 ID	必填	/	长整型	退回的机房 ID
2	gatewayId	互联网出入口 ID	选填	/	长整型	退回的机房链路 ID
3	ipSegId	IP 段 ID	选填	/	长整型	退回的机房 IP 段 ID
4	frameInfoId	机架信息	选填	/	长整型	退回的机房机架 ID

表 50 退回的用户数据（节点：user）

编号	节点	节点名称	子节点	子节点名称	必填	数据类型	长度	描述
1	userId	用户 ID	/	/	必填	长整型	32	退回的用户 ID 或者要从中退回应用服务/应用服务域名/占用机房信息的用户 ID
2	service	退回的应用服务数据 <sup>a</sup>	serviceId	应用服务 ID	必填	长整型	/	退回的应用服务 ID 或者要从中退回应用服务域名及占用机房信息的应用服务 ID
			domainId	应用服务的	选填	长整型	/	退回的应用服务域名 ID（应用

			域名 ID				服务 ID 必填)
	hhId	占用机房信息 ID	/	/	选填	长整型	/ 退回的占用机房信息 ID (应用服务 ID 必填)
3	hhId	占用机房信息 ID	/	/	选填	长整型	/ 退回的占用机房信息 ID

<sup>a</sup> 该节点选填

#### 11.15 免过滤网站列表指令内容

表 51 免过滤域名列表指令（节点：noFilter）

编号	节点	节点名称	必填	数据类型	长度	描述
1	commandId	指令 ID	必填	长整型	4	指令惟一 ID，该 ID 由 SMMS 产生
2	idcId	IDC/ISP 经营者 ID	必填	字符串	18	电信管理部门颁发的 IDC/ISP 许可证号
3	operationType	操作类型	必填	整型	/	对该记录的操作类型，包括： 0——新增； 1——删除
4	type	类型	必填	整型	/	1-域名 2-IP
5	contents	列表内容	必填	字符串	128	域名或 IP 地址
6	level	指令优先级	必填	字符串	12	见表 10.10 节，二进制代码
7	timeStamp	生成时间	必填	字符串	19	生成该查询指令的时间

#### 11.16 违法网站列表指令内容

表 52 违法网站列表指令（节点：blacklist）

编号	节点	节点名称	必填	数据类型	长度	描述
1	commandId	指令 ID	必填	长整型	4	指令惟一 ID，该 ID 由 SMMS 产生
2	idcId	IDC/ISP 经营者 ID	必填	字符串	18	电信管理部门颁发的 IDC/ISP 许可证号
3	operationType	操作类型	必填	整型	/	对该记录的操作类型，包括： 0——新增； 1——删除
4	type	类型	必填	整型	/	1-域名 2-IP
5	contents	列表内容	必填	字符串	128	域名或 IP 地址
6	level	指令优先级	必填	字符串	12	见表 10.10 节，二进制代码
7	timeStamp	生成时间	必填	字符串	19	生成该查询指令的时间

#### 11.17 活跃资源监测数据上报内容

IDC/ISP 活跃资源监测数据包括活跃的域名信息、活跃 IP 地址信息。

表 53 在线活跃资源数据信息上报（节点：activeResources）

编号	节点	节点名称	必填	长度	描述
1	findDomainList	在线活跃的域名信息	选填	/	见表 54（可重复多次）
2	findIpList	在线活跃的 IP 地址信息	选填		见表 55（可重复多次）

表 54 在线活跃的域名信息上报数据格式（节点：findDomainList）

编号	节点	节点名称	是否必填	长度	数据类型	描述
1	findDomainListDomain	在线活跃的本级域名	必填	128	字符串	在线活跃的本级域名

2	findDomainListFirstTime	首次采集时间	必填	20	字符串	采用 yyyy-MM-dd HH: mm:ss 格式
3	findDomainListLastTime	最后活跃时间	必填	20	字符串	采用 yyyy-MM-dd HH: mm:ss 格式
4	block	是否阻断	必填	1	整型	有域名或 IP 在违法网站列表中、或是触发过滤规则，对此类资源的访问既触发阻断，0: 未阻断 1: 阻断
5	visitsCount	访问量	必填	/	长整型	当 topDomainflag 节点为 0 时，记录顶级域名当天累积的访问量，当为 1 时，记录非顶级域名当天累积的访问量
6	topDomainflag	顶级域名标记	必填		整形	顶级域名指除根以外带有一个“.”的域名，即通用顶级域（gTLD），国家（地区）代码顶级域（ccTLD），国际化顶级域（IDN TLD）的一级域名，0: 顶级域名，1: 非顶级域名
7	topDomain	相应顶级域名	可填		字符串	顶级域名，topDomainflag 为 1 时，必填
8	ip	对应 IP 地址	必填		字符串	对应 IP 地址 <u>±（专线）</u>
9	idcId	IDC/ISP 经营者 ID	必填	128	字符串	IDC/ISP 经营者 ID
10	houseId	机房 ID	必填		长整型	机房 ID

表 55 在线活跃的 IP 地址信息上报数据格式(节点: findIpList)

编号	节点	节点名称	必填	长度	数据类型	描述
1	findIpListIp	在线活跃的 IP 地址	必填	128	字符串	在线活跃的 IP 地址 <u>±</u>
2	findIpListFirstTime	首次采集时间	必填	20	字符串	采用 yyyy-MM-dd HH:mm:ss 格式
3	findIpListLastTime	最后活跃时间	必填	20	字符串	采用 yyyy-MM-dd HH:mm:ss 格式
4	block	是否阻断	必填	1	整型	有域名或 IP 在违法网站列表中、或是触发过滤规则，对此类资源的访问既触发阻断，0: 未阻断 1: 阻断
5	visitsCount	访问量	必填	/	长整型	访问量
6	isInIpSeg	报备状态	必填	1	整型	报备状态：指企业侧系统将数据是否已上报 SMMS 的状态 0: 已上报 SMMS，1: 未上报 SMMS
7	port	应用端口	必填		长整型	应用端口
8	protocol	传输层协议类型	必填	整型	/	1-TCP 2-UDP

**批注 [钱康6]:** 对于专线资源上报的活跃域名，需要在该字段添加（专线）标识  
例：192.168.1.1(专线)

**批注 [钱康7]:** 对于专线资源上报的活跃域名，需要在该字段添加（专线）标识  
例：192.168.1.1(专线)



9	idcId	IDC/ISP 经营者 ID	必填	128	字符串	IDC/ISP 经营者 ID
10	houseId	机房 ID	必填		长整型	机房 ID

### 11.18 违法违规网站监测数据上报内容

ISMS 将所有监测到的违法违规网站信息数据主动上报给 SMMS。每日上报一次。

表 56 违法违规网站监测数据(节点: illegalWeb)

编号	节点	节点名称	必填	数据类型	长度	描述
1	idcId	IDC/ISP 经营者 ID	必填	字符串	128	IDC/ISP 经营者 ID
2	houseId	机房 ID	必填	长整型	/	机房 ID
3	domain	违法违规域名	选填	字符串	128	监测到的实际域名
4	ip	域名对应的 IP 地址	必填	字符串	64	监测到的域名对应的 IP 地址
5	port	端口	必填	长整型	/	监测到的目的端口
6	serviceContent	服务内容	必填	整形	/	填写服务的内容, 见 10.6 节 (可重复多次)
7	illegalType	违法违规情况	必填	整型	/	违法违规的情况, 见 10.8 节
8	firstFound	首次发现时间	必填	字符串	19	首次监测到该异常的时间, 采用 yyyy-MM-dd HH:mm:ss 格式
9	lastFound	最近一次发现时间	必填	字符串	19	当天最后一次发现该异常的时间, 采用 yyyy-MM-dd HH:mm:ss 格式
10	visitCount	24 小时累积访问量	必填	长整型		该域名的访问次数统计
11	protocol	传输层协议类型	必填	整型		1-TCP 2-UDP
12	block	是否阻断	必填	整形	1	0: 未阻断 ,1:阻断
13	operationAccount	处置人账号	必填	字符串		处置人账号为实施处置操作的用户登录名, 如根据 SMMS 指令自动处置则记录为“ISMS”, 如未处置则记录为空。

### 11.19 活跃资源访问量查询指令内容

SMMS 查询 ISMS 在线活跃的顶级域名或者子域名的当天累积访问量, 查询起始时间默认为每天的 00:00:00, 查询截至时间默认为指令建立的当前时间。

表 57 活跃资源访问量查询指令格式及描述 (节点: queryView)

编号	节点	节点名称	必填	数据类型	长度	描述
1	commandId	指令 ID	必填	长整型	4	指令惟一 ID, 该 ID 由 SMMS 产生
2	idcId	IDC/ISP 经营者 ID	必填	字符串	128	电信管理部门颁发的 IDC/ISP 许可证号
3	type	查询类型	必填	整型		1-顶级域名 2-子域名 统计自身域名的访问量
4	content	查询内容	必填	字符串	512	根据查询类型 type 节点填写相对应的内容
5	queryTime	查询截至时间	必填	字符串	19	查询截至时间默认为当前时间
6	timeStamp	生成时间	必填	字符串	19	生成该查询指令的时间

### 11.20 违法管理指令执行记录指令

SMMS 查询 ISMS 系统中曾经执行过的监测或者过滤指令, 累积执行成功的计数。

表 58 违法管理指令执行记录指令格式及描述 (节点: commandRecord)

编号	节点	节点名称	必填	数据类型	长度	描述
1	commandId	指令 ID	必填	长整型	4	管理指令的惟一编码, 由

						SMMS 产生
2	idcId	IDC/ISP 经营者 ID	必填	字符串	128	电信管理部门颁发的 IDC/ISP 许可证号
3	controlsId	违法信息安全管理指令 ID	必填	长整型	/	违法信息安全管理指令 ID
4	timeStamp	生成时间	必填	字符串	19	生成该查询指令的时间

中国信息通信研究院