ICS 35.020
L 70

团　　体　　标　　准

T/DSAG 001-2025

数字政府视频云网边界安全技术标准

(Digital Government Video Cloud Network Boundary Security Technical Standard)

2025 - 01 - 01 发布　　2025 - 01 - 01 实施

广东省数字安全协会　　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由广东省数字安全协会归口管理。

本文件起草单位：深信服科技股份有限公司、杭州迪普科技股份有限公司、广州天懋信息系统股份有限公司、杭州安恒信息技术股份有限公司、广州智臣信息科技有限公司、广东科城信服信息技术有限公司。

本文件主要起草人：常晓宇、常伟、邹凯、何锐坚、吕涛、黄福印、曾磊、赵阳、刘吉林、武进、刘俊强、王景。

数字政府视频云网边界安全技术标准

1 范围

本文件规定了广东省数字政府视频云网边界的安全策略和能力要求等。

本文件适用于广东省数字政府各部门云网边界安全交互的规划设计、部署实施、检测验收和运行维护。

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 22239-2019 信息安全技术 网络安全等级保护基本要求

GW 0205-2014 国家电子政务外网跨网数据安全交换技术要求与实施指南

GW 0206-2014 接入政务外网的局域网安全技术规范

GB/T28181 公共安全视频监控联网系统信息传输、交换、控制技术要求

GB 35114 公共安全视频监控联网信息安全技术要求

GA/T1788.1-2021 公安视频图像信息系统安全技术要求第 1 部分:通用要求

GA/T1788.3-2021 公安视频图像信息系统安全技术要求第 3 部分:安全交互

3 术语和定义

下列术语和定义适用于本文件。

数字政府视频监控平台 video surveillance platform for digital government

由部门或行业建设的、实现视频图像联网并提供视频监控综合管理服务的软件和硬件。

数字政府视频共享交换平台 video sharing and exchanging platform for digital government

对各部门视频监控平台的实时视频流（或录像文件）进行接入和共享交换的软件与硬件。

视频云网边界安全交互系统 boundary security interactive system for video cloud network

在数字政府视频网络边界建立的实现视频图像信息交互安全机制的软件与硬件。

横向视频云网边界安全交互系统 horizontal border security interaction system

数字政府视频共享交换平台与其他数字政府视频监控平台互联时建立信息交互安全机制的软件与硬件。

纵向视频云网边界安全交互系统 vertical access security interaction system

数字政府视频共享交换平台纵向级联时建立信息交互安全机制的软件与硬件。

物理隔离 Physical isolation

物理隔离是指采用物理方法将不同安全等级网络隔离从而避免入侵或信息泄露风险的技术手段。

逻辑隔离 Logic isolation

逻辑隔离是指采用技术方法将不同安全等级网络隔离从而避免入侵或信息泄露风险的技术手段，被隔离的两端仍然存在物理上数据通道连线。

4 符号与缩略语

下列缩略语适用于本文件。

API：应用程序接口（Application Programming Interface）

DDoS：分布式拒绝服务（Distributed Denial of Service）

FTP：文件传输协议（File Transfer Protocol ）

ID：身份标识（Identity Document）

IP：因特网协议（Internet Protocal）

JDBC：Java 数据库连接（Java Database Connectivity ）

MAC：媒体存取控制位址（Media Access Control Address）

SNMP:简单网络管理协议（Simple Network Management Protocol）

Syslog:系统记录（Syslog）

TCP: 传输控制协议（Transmission Control Protocol）

UDP: 用户数据报协议（User Datagram Protocol）

SIP: 会话初始协议(Session Initiation Protocol)

5 数字政府视频云网边界安全交互系统架构

5.1 数字政府视频云网边界安全交互体系

视频云网边界安全交互系统分为横向视频云网边界安全交互系统和纵向视频云网边界安全交互系统，结构框图见图1。

数字政府视频共享交换平台应设置横向视频云网边界安全交互系统，通过电子政务外网对接同级部门或行业视频监控平台，对横向视频交换进行安全防护。支持互联网、与互联网逻辑隔离网络、与互联网物理隔离网络等网络类型。

上级数字政府视频共享交换平台应设置纵向视频云网边界安全交互系统，通过电子政务外网纵向级联下级数字政府视频共享交换平台，对跨级视频交换进行安全防护。纵向视频云网边界安全交互系统不隔离路由，上下级系统之间应用路由可达。纵向连接应采用符合GB/T28181、GB 35114-2017 等的视频流和其他必要的远程访问、运维和安全服务的交互。

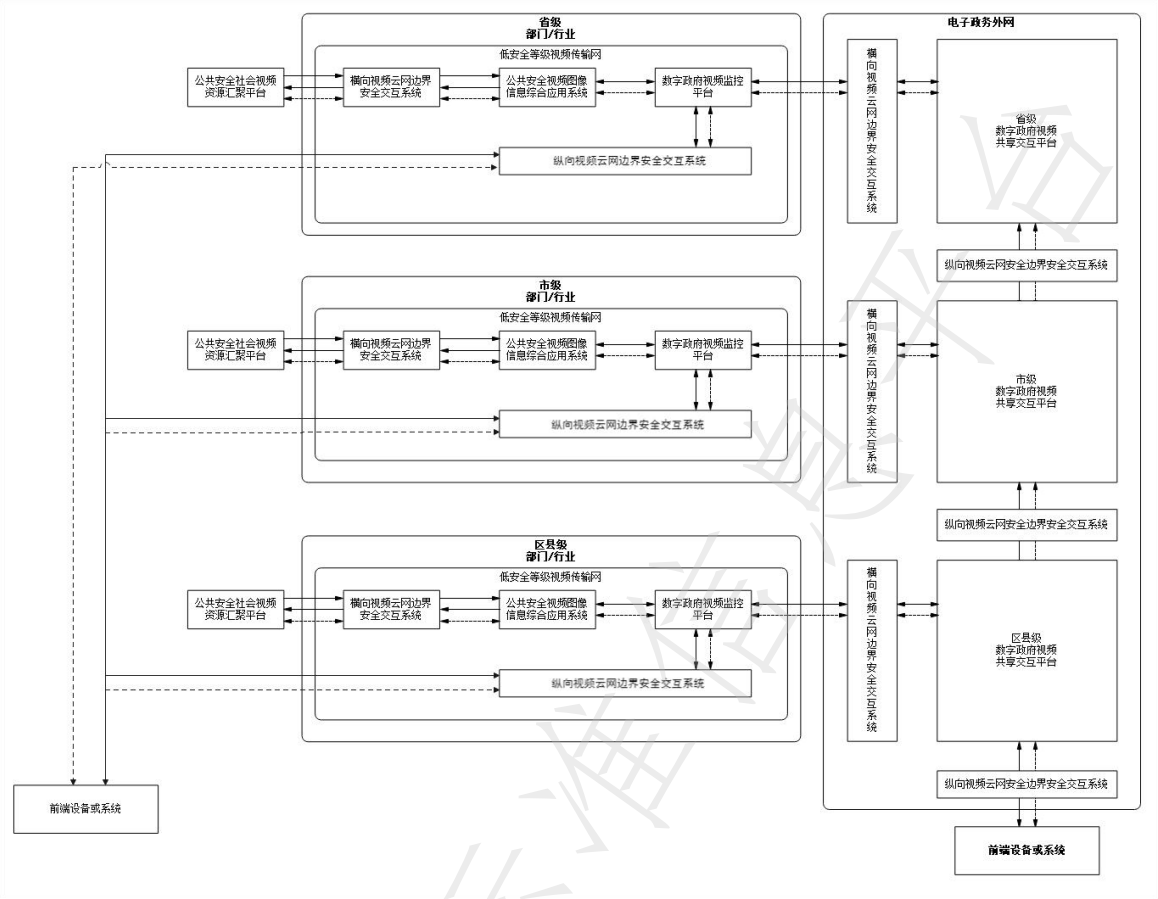

图 1 视频云网边界安全交互系统结构框图

5.2 横向视频云网边界安全交互系统功能架构

5.2.1 功能架构

横向视频云网边界安全交互系统功能架构见图 2，共包含五个安全域：路由接入区、边界保护区、应用服务区、安全隔离区和安全监测与管理区，每个安全区域实现不同的安全功能。

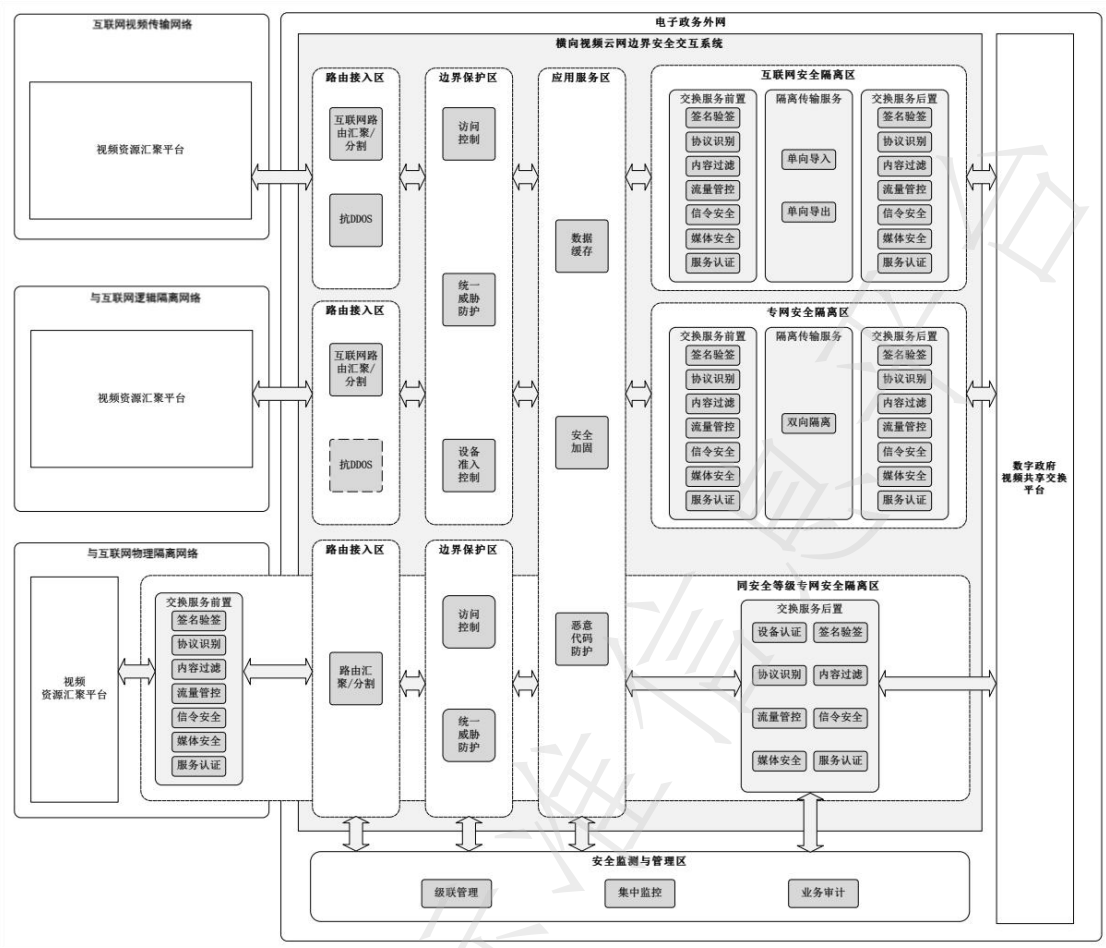

图 2 横向视频云网边界安全交互系统功能架构图

5.2.2 路由接入区

路由接入区将各外部链路与横向视频云网边界安全交互系统连接。实现路由访问控制，将来自不同接入对象或不同外部链路的视频流按照不同的安全策略加以区分，对于互联网接入应支持抗DDOS攻击能力。

5.2.3 边界保护区

边界保护区主要实现对横向视频云网边界安全交互系统的边界保护，应支持的主要安全功能为：实现访问控制、设备准入和统一威胁防护，包括网络入侵防护和网络恶意代码防护等安全能力。

5.2.4 应用服务区

应用服务区主要处理各类与应用相关的操作，是对外信息发布、信息采集和数据交换的中间区域，应支持数据暂存、安全加固、恶意代码防护等功能。在视频交换中，一般不强制要求建立应用服务区。

5.2.5 安全隔离区

安全隔离区实现**数字政府视频共享交换平台**与互联网、**与互联网逻辑隔离网络、与互联网物理隔离网络内的数字政府视频监控平台之间**的安全隔离与信息交换，主要包括：

a) 针对互联网视频接入和共享，安全隔离区提供单向导入、单向导出、签名验签、协议识别、内容过滤、流量管控、服务认证、信令安全、媒体安全等安全能力。其中视频流采用单向传输的方式。

b) 针对与互联网逻辑隔离网络的视频交换，安全隔离区提供双向隔离、签名验签、协议识别、内容过滤、流量管控、服务认证、信令安全、媒体安全等安全能力。

c) 针对与互联网物理隔离网络的视频交换，安全隔离区提供设备认证、签名验签、协议识别、内容过滤、流量管控、服务认证、信令安全、媒体安全等安全能力。与互联网物理隔离网络与数字政府视频共享交换平台互联时，可根据实际需要选择是否采用安全隔离设备进行网络隔离。

5.2.6 安全监测与管理区

安全监测与管理区实现横向视频云网边界安全交互系统的业务审计、集中监管与级联上报等。应支持以下主要安全功能：

a) 对各个安全组件的日志和交换业务日志进行采集；

b) 对横向视频云网边界安全交互系统的资产信息、安全基线、策略配置、运行状态进行集中监控；

c) 向上级平台级联上报本级系统的数据。

5.3 纵向视频云网边界安全交互系统功能架构

5.3.1 功能架构

纵向视频云网边界安全交互系统划分为安全防护区和安全监测与管理区，系统功能架构见图3。

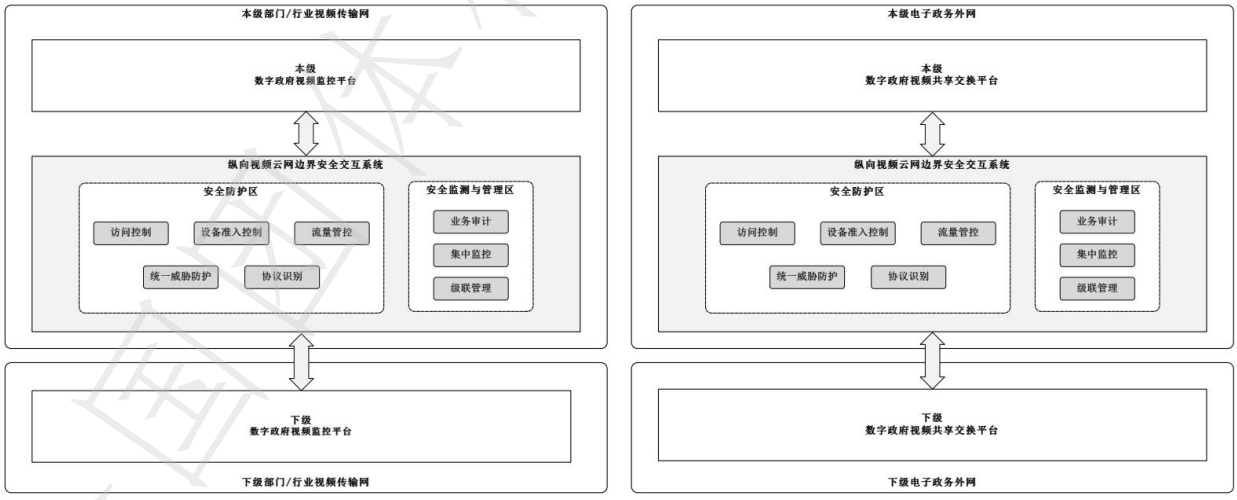

图 3 纵向视频云网边界安全交互系统功能架构图

5.3.2 安全防护区

安全防护区应支持下级**数字政府视频共享交换平台**与上级**数字政府视频共享交换平台**进行可控的信息交换，应满足以下要求：

a) 对下级数字政府视频共享交换平台，安全防护区提供访问控制、统一威胁防护、设备准入、协

议识别和流量管控等安全能力，应支持符合 GB/T28181、GB 35114-2017 等的视频流和其他必要的远程访问、运维和安全服务协议的交互。

b) 社会视频资源前端设备采用专线方式与数字政府视频共享交换平台直接互联时，宜采用社会资源安全联网设备与平台相连。

5.3.3 安全监测与管理区

安全监测与管理区应实现纵向视频云网边界安全交互系统的业务审计、集中监管与级联上报等，可以与横向视频云网边界安全交互系统共用，满足以下安全功能要求：

a) 支持对各个安全组件的日志和交换业务日志进行采集；

b) 支持对纵向视频云网边界安全交互系统的资产信息、安全基线、策略配置、运行状态进行集中监控；

c) 支持向上级平台级联上报本级系统的数据。

6 视频云网边界安全能力要求

6.1 访问控制

应支持通过基于会话的防护规则实现网络访问控制。对不符合规则的访问，系统应进行拦截并发出告警。

6.2 设备准入控制

设备准入控制满足以下要求：

c) 应支持全流量的检测及处理能力，对非授权设备的信令和媒体流量进行实时阻断并发出告警；

d) 应支持接入平台的信息注册，注册信息应包括设备 IP/MAC、设备 ID、设备属性等信息；

e) 应具备实时阻断重放攻击、中间人攻击等攻击的能力；

f) 准入控制设备宜支持通过公钥基础设施为设备颁发身份证书，确保经过核验的设备具有公钥基础设施颁发的设备身份证书；

g) 宜支持采集接入设备的硬件信息、操作系统补丁状态、病毒库、进程、注册表、账户等信息，为信任评估提供实时准确的设备环境信息；

h) 宜通过环境感知或基于硬件安全模块的环境完整性度量等技术，感知设备运行环境和状态的能力。

6.3 统一威胁防护

支持通过检测、阻断、限流、审计报警等防御手段，对蠕虫、后门、木马、间谍软件、Web 攻击、APT 等攻击形式进行有效防御。

6.4 抗 DDoS 攻击防护

支持通过指纹特征识别，攻击源认证，智能协议分析等多种手段有效地阻断各种带宽型 Flood 攻击、连接型慢速攻击及针对 SIP 应用的 DDoS 攻击。

6.5 安全加固

通过补丁修复、安装脚本、调整配置等方式增强系统的健壮性，防范或阻断恶意攻击，提升系统安全性。

6.6 恶意代码防护

支持通过恶意代码检测引擎和恶意代码库的技术融合，对恶意代码进行高效检测和防御。

6.7 签名验签

签名验签应满足以下要求：

a) 应采用统一密钥基础设施签发的数字证书对视频信源进行签名验签，确保视频信源的真实性、完整性和不可抵赖性；

b) 应支持对统一密钥基础设施的验签服务进行接口调用，对视频信源进行签名验证；

c) 应支持对无签名或签名验证失败的视频信源进行拦截丢弃，并进行日志报警。

6.8 协议识别

支持对指定协议的信令和视频流基于安全策略进行格式检查，对不符合格式的信令和视频流进行拦截丢弃，并发出进行告警。

6.9 内容过滤

内容过滤应满足以下要求：

a) 支持对指定协议的信令和数据流基于安全策略进行内容过滤，对含有敏感信息的信令进行阻断，并发出日志报警；

b) 纵向安全服务交互系统应支持对 API 请求/响应报文数据基于安全策略进行内容过滤，对含有敏感信息的 API 报文数据进行阻断，并发出日志报警。

6.10 流量管控

支持对视频流量进行监测，以规则或统计基线判定异常并实施控制并发出告警。

6.11 服务认证

纵向视频云网边界安全交互系统服务认证应满足以下要求：

a） 支持通过鉴权方式对服务调用方进行身份认证，认证凭证包括数字证书、口令密码、动态令牌等；

b） 支持对服务调用方进行权限控制，确保最小授权；

c） 支持对服务提供注册、编目、查询、变更、注销等功能。

6.12 信令安全

支持采用信令加签、信令加密等手段保证信令协议自身安全，抵御信令被篡改、夹带、窃听等安全风险。

6.13 媒体安全

支持采用媒体流加签、媒体流加密等手段保证媒体流协议自身安全，抵御媒体流被篡改、夹带、窃听等安全风险。

6.14 单向导入/导出

单向导入/导出应满足以下要求：

a） 应采用物理光通路建立单向传输通道，确保无任何反向通道；

b） 应对视频流单向传输过程提供完整的日志记录；

c） 单向导入/导出设备应提供身份鉴别、访问控制等基础能力。

d） 单向导入/导出设备应支持通过标准管理接口、应用服务或协议，实现与第三方集中监控与管理系统的级联与接入管理。

6.15 双向隔离

双向隔离应满足以下要求：

a) 应通过摆渡方式连接网络内外两侧，支持通过物理隔离方式断开内外部连接；

b) 应支持根据事先定义的安全策略，对视频协议头部信息的剥离与封装；

c) 应对视频流双向传输过程提供完整的日志记录；

d) 双向隔离通道设备应提供身份鉴别、访问控制等基础能力。

e) 应支持对数据格式、数据内容进行检查和过滤；

f) 双向隔离通道设备应支持通过管理接口、应用服务或协议，实现与第三方集中监控与管理系统的接入与级联管理。

6.16 业务审计

业务审计满足以下要求：

a） 支持以 Syslog、JDBC、FTP、API 接口等方式采集业务日志数据；

b） 支持将采集到的所有安全组件日志向管理端进行报送。

6.17 集中监控

集中监控与管理应满足以下要求：

a） 应支持边界安全交互系统运行状态监控，具备安全交互系统相关设备、链路、业务运行状态的监控能力；

b） 应支持边界安全交互系统相关的设备资产管理，资产信息包括设备类型、品牌型号、操作系统、版本、端口等信息，并支持资产注册功能；

c） 应支持边界安全交互系统基线管理，具备运行状态监控、安全审批等能力；

d） 应支持边界安全交互系统策略管理，具备安全策略配置下发、变更、删除、查询等能力；

e） 应支持边界安全交互系统审计数据集中收集和存储，具备异常事件分析、追踪、溯源和处理等能力；

f） 应支持通过管理接口、应用服务或协议，具备与第三方边界安全交互系统各安全组件的对接及接入管理的能力；

g） 宜提供对边界安全交互系统的级联管理，具备管理数据报送、审批、通报等能力。