



中华人民共和国国家标准

GB/T 24294.1—2026

代替 GB/Z 24294.1—2018

网络安全技术 基于互联网电子政务信息安全实施指南 第 1 部分：总则

Cybersecurity technology—Guide of implementation for internet-based
e-government information security—Part 1: General

2026-04-30 发布

2026-11-01 实施

国家市场监督管理总局
国家标准化管理委员会 发布

目 次

前言	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	2
5 参考模型	2
5.1 模型框架	2
5.2 安全策略	3
5.3 需求识别	3
5.4 安全设计	3
5.5 安全实施	4
5.6 运行与评估	4
5.7 系统迁移与废止	4
6 技术体系	5
6.1 概述	5
6.2 边界防护	5
6.3 设备接入安全与安全通信网络	5
6.4 政务云服务安全	6
6.5 政务数据安全	6
6.6 政务云应用安全	6
6.7 权限安全管控	6
6.8 安全审计	6
7 体系实施原则	7
7.1 按需保护原则	7
7.2 权限最小化原则	7
7.3 系统分域控制原则	7
7.4 动态防护原则	7
7.5 残余信息保护原则	7
7.6 供应链安全原则	7
8 体系实施框架	7
8.1 传统业务部署模式下的体系实施框架	7
8.2 云计算部署模式下的体系实施框架	9

9 密码使用与安全保密职责..... 10

9.1 密码使用 10

9.2 安全保密职责 10

参考文献 11

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。

本文件是 GB/T 24294《信息安全技术 基于互联网电子政务信息安全实施指南》的第1部分。《信息安全技术 基于互联网电子政务信息安全实施指南》已经发布了以下部分：

- 第1部分：总则；
- 第2部分：接入控制与安全交换；
- 第3部分：身份鉴别与授权管理；
- 第4部分：终端安全防护。

本文件代替 GB/Z 24294.1—2018《信息安全技术 基于互联网电子政务信息安全实施指南 第1部分：总则》。与 GB/Z 24294.1—2018 相比，除结构调整和编辑性改动外，主要技术变化如下：

- a) 更改了基于互联网电子政务信息安全参考模型(见第5章,2018版的第5章)；
- b) 更改了基于互联网电子政务信息安全技术体系(见第6章,2018版的第6章)；
- c) 更改了体系的实施原则(见第7章,2018版的第7章)；
- d) 更改了体系的实施架构(见第8章,2018版的第8章)；
- e) 增加了第9章“密码使用与安全保密职责”(见第9章)；
- f) 删除了体系的风险评估(见2018版的第10章)。

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专利的责任。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中国人民解放军网络空间部队信息工程大学、国家信息中心、北京市经济和信息化局网络安全管理中心、郑州云智信安安全技术有限公司、北京天融信网络安全技术有限公司、华中科技大学、北京神州绿盟科技有限公司、郑州信大捷安信息技术股份有限公司、武汉民为技术有限公司、广州卓腾科技有限公司。

本文件主要起草人：陈性元、杜学绘、任志宇、王娜、曹利峰、王文娟、张东巍、孙奕、单棣斌、刘敖迪、刘莺迎、刘蓓、闫桂勋、李媛、张乾坤、张楠、郜军伟、彭铭、王宇、陈卓、刘瑶、景鸿理、罗元、谢琴、张超、王浩宇、董枫、赵彦杰、叶晓虎、范敦球、黄俊、叶建伟、廖正赞、梅光明、曹婉玉。

本文件及其所代替文件的历次版本发布情况为：

- 2009年首次发布为 GB/Z 24294—2009；
- 2018年第一次修订为 GB/Z 24294.1—2018；
- 本次为第二次修订。

引 言

互联网电子政务服务是一种依托互联网面向公众用户、企业法人、远程政务人员提供的便捷可靠的政务服务模式,主要服务于广大群众民生、企业用户营商、移动人员办公等领域,但面临着身份假冒、网络攻击、非授权访问和信息泄漏等安全威胁。为推进一体化政务服务平台在地市(含以下)单位的应用,指导地市级(含以下)单位的互联网电子政务安全保障工作,特制定本文件。

《网络安全技术 基于互联网电子政务信息安全实施指南》拟由四个部分构成。

- 第1部分:总则。目的在于给出基于互联网电子政务信息安全的参考模型、网络安全技术体系、体系实施原则、体系实施框架和密码使用与安全保密职责。
- 第2部分:接入控制与安全交换。目的在于明确互联网电子政务分域控制的二个阶段,在接入控制阶段,对接入控制结构、接入安全设备功能、接入认证、接入控制规则、接入控制管理等方面给出指南性建议;在安全交换阶段,对安全交换模式、定制数据安全交换要求、数据流安全交换要求给出指南性建议。
- 第3部分:身份鉴别与授权管理。目的在于明确互联网电子政务信息安全系统中的身份鉴别与授权管理功能,对身份鉴别与授权管理技术实施给出指南性建议。
- 第4部分:终端安全防护。目的在于明确基于互联网电子政务终端的安全功能、实施原则和应用模式,对终端基本安全防护、终端增强安全防护、移动终端安全防护给出指南性建议。

网络安全技术

基于互联网电子政务信息安全实施指南

第1部分：总则

1 范围

本文件给出了基于互联网电子政务信息安全的参考模型、网络安全技术体系、体系实施原则、体系实施框架和密码使用与安全保密职责。

本文件适用于地市级(含以下)政府单位的互联网电子政务网络安全建设与运维,为地市级(含以下)政府单位开展一体化政务服务平台建设及安全保障提供依据。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 22239	信息安全技术	网络安全等级保护基本要求
GB/T 22240	信息安全技术	网络安全等级保护定级指南
GB/T 30272	信息安全技术	公钥基础设施 标准符合性测评
GB/T 31167	信息安全技术	云计算服务安全指南
GB/T 31168	信息安全技术	云计算服务安全能力要求
GB/T 35273	信息安全技术	个人信息安全规范
GB/T 35274	数据安全技术	大数据服务安全能力要求
GB/T 36637	信息安全技术	ICT 供应链安全风险管理指南
GB/T 37092	信息安全技术	密码模块安全要求
GB/T 37973	信息安全技术	大数据安全管理指南
GB/T 39786	信息安全技术	信息系统密码应用基本要求
GB/T 43698	网络安全技术	软件供应链安全要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

互联网政务服务 internet-based government services

各级政务服务机构运用互联网、大数据和云计算等技术,构建“互联网+政务服务”平台,整合各类政务服务事项和业务办理等信息,为自然人和组织提供一站式办理的政务服务。

3.2

安全政务办公 secure government affairs

通过数据分域存储、统一身份鉴别、统一授权管理和信息分类防护等安全技术,与电子政务办公应

用相结合的服务方式。

3.3

可信政务服务 trusted government services

通过数据分域存储、统一身份鉴别和网页防篡改等安全技术,与政务服务相结合的服务方式。

3.4

基于互联网电子政务网络安全系统 cybersecurity system of e-government network based on internet

针对基于互联网的电子政务网络环境,综合运用多种安全技术和管理措施,以保障电子政务网络及其承载的信息、数据和政务业务的安全系统。

4 缩略语

下列缩略语适用于本文件。

App:应用程序(application)

API:应用编程接口(application programming interface)

DDoS:分布式拒绝服务(distributed denial of service)

IPSec:网络安全协议(IP security protocol)

PKI:公钥基础设施(public key infrastructure)

SSL:安全套接字层(secure sockets layer)

VPN:虚拟专用网络(virtual private network)

5 参考模型

5.1 模型框架

基于互联网电子政务网络安全参考模型框架见图 1。

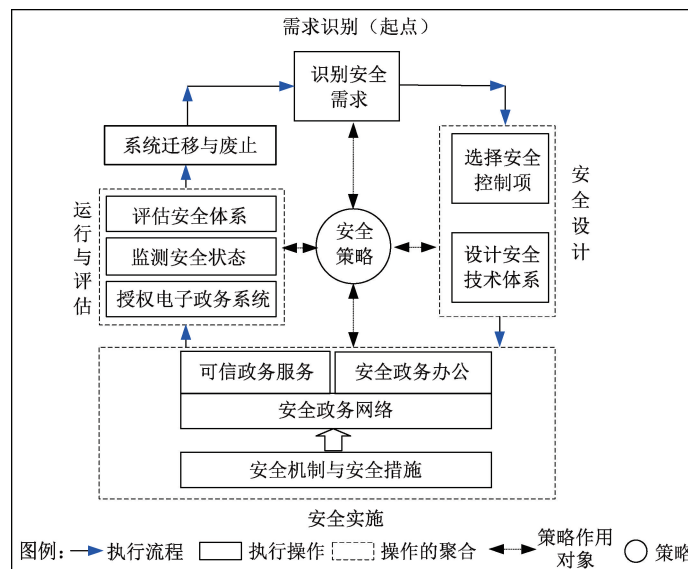


图 1 参考模型框架

基于互联网电子政务网络安全参考模型由“需求识别—安全设计—安全实施—运行与评估—系统迁移与废止”五个阶段组成,该模型以安全策略为中心,通过识别、设计、实施、评估和废止,对基于互联网电子政务网络安全系统进行全生命周期的建设与运维。

5.2 安全策略

安全策略是用于所有与安全相关活动的一套规则,在参考模型中处于核心地位,宜能够根据系统所面临的风险与需求进行动态调整与优化,以适应不断变化的网络安全形势。

它是安全互联设备、接入控制设备、安全交换装置、终端安全防护设备和鉴别授权设备等各类安全设备所设置的安全规则,是实施权限管理与访问控制的依据。在基于互联网电子政务系统中,宜根据系统中所发生的攻击事件、入侵行为,以及业务、数据等用户访问行为,调整网络安全设备中的安全防护规则。

5.3 需求识别

5.3.1 安全对象识别

互联网电子政务应用是安全保护的對象,安全对象包括如下两类:

- a) 政务办公:政府部门内部的业务处理,如政府部门间的公文流转、公文处理、办公管理和数据共享等;
- b) 政务服务:通过网上大厅、办事窗口、移动客户端和自助终端等多种形式,结合第三方平台,面向社会公众所提供的一站式政务服务,包括信息公开、社保医保、婚姻生育和互动交流等服务内容。政务服务的形态包括政务网站、政务 App 和政务小程序等。

5.3.2 政务数据识别

在地市级(含以下)基于互联网电子政务系统中,不涉及国家电子政务秘密,政务数据包括如下两类:

- a) 内部数据:内部数据是面向政府部门内部人员按级、按范围、按单位可访问的信息,如政务办公文件、政务共享数据和政务会议通知等;
- b) 公开数据:公开数据是在互联网上可以向公众开放的信息,如政务服务流程、政务信息公示、公众服务项目和企业服务信息等。

5.3.3 安全目标识别

安全目标识别包括如下内容:

- a) 政务办公及其内部信息的安全防护重点主要包括对政务人员的身份鉴别、政务资源的授权访问和数据传输保护等方面;
- b) 政务办公及其内部信息的安全防护重点主要为应用系统及其信息的完整性和可用性,以及隐私信息的机密性,以防范数据的非法修改、隐私信息的泄露,政务办公所包含的内部信息主要包括政府重要公文、政府重要计划、企业审批事项和个人隐私信息等。

5.3.4 安全保护等级识别

按 GB/T 22240 对基于互联网电子政务系统进行安全保护等级识别,按 GB/T 22239 进行安全框架构建。

5.4 安全设计

5.4.1 选择安全控制项

根据基于互联网电子政务系统的应用范围、应用模式、安全要求与期望,以及所采用的云计算、大数据和传统数据库等应用技术,选择合适的安全技术与安全控制项,按第 6 章和第 8 章构建对应的基于互

联网电子政务网络安全实施框架。

5.4.2 设计安全技术体系

为保障基于互联网电子政务系统中的安全应用(包括安全政务办公、可信政务服务两类),实现政务信息在互联网上的安全传输,宜依托 PKI 所提供的数字证书等服务,通过综合采用以密码为核心的安全技术,从边界防护、设备接入安全与安全通信网络、政务云服务安全、政务数据安全和政务云应用安全,到权限安全管控、安全审计,形成一体化安全防护体系。

5.5 安全实施

在基于互联网电子政务系统识别的基础上,根据安全策略,依据所设计的安全技术体系,构建安全机制与安全措施,宜从政务网络、政务办公和政务服务三个方面,构建安全政务网络、安全政务办公平台和可信政务服务平台,对基于互联网电子政务系统进行安全保护,具体如下:

- a) 采用密码、防火墙、VPN 和微隔离等技术,依托互联网,通过有线、无线等多种手段,在各接入单位与政务服务中心之间形成虚拟的安全政务网络;
- b) 采用政务人员身份鉴别、政务资源授权访问和政务信息分类保护等技术,对政务部门内部的业务处理系统(如政务办公、政务审批管理等)进行安全保护,实现安全的政务办公;
- c) 采用政务人员身份鉴别、政务信息发布审核和政务服务可靠运行等安全技术,对一站式政务服务平台进行安全保护,实现可信的政务服务;
- d) 对公众人员、企业法人等政务服务对象,宜通过实名注册、身份鉴别、口令或令牌登录和后台权限控制等方式,实现便捷与可靠的一体化政务服务。

5.6 运行与评估

5.6.1 授权电子政务系统

根据基于互联网电子政务系统的安全风险评估报告,确定电子政务系统当前安全状态及其安全风险在可授权的范围内,批准电子政务系统继续运行,并同时授权组织定期测试,评估安全策略、安全技术和运行措施的有效性。

5.6.2 监测安全状态

通过系统识别、安全监控、监视分析、安全审计和态势感知等手段,实时监控互联网电子政务系统中网络和主机活动、监视分析用户与系统行为、统计跟踪网络异常行为、识别违反安全策略的行为,使管理人员能够有效监管、控制和评估互联网电子政务系统中的安全行为。

5.6.3 评估安全体系

针对建设或运行中的互联网电子政务系统,采用分析、验证、核查、扫描检测和渗透测试等手段,依据等级保护、密码应用和云应用等相关国家标准开展安全评估,对系统进行符合性验证与安全风险评估,使各项安全机制符合基于互联网电子政务网络安全实施要求,降低网络安全风险。

安全评估一般包括建设项目验收评估及运行期间的定期评估两种。在对基于互联网电子政务系统进行安全评估后,给出网络安全评估报告,并针对网络安全风险评估的结果,对基于互联网电子政务系统进行安全整改。

5.7 系统迁移与废止

互联网电子政务系统在终止或部分终止前,包含数据的系统、设备或存储媒体等按安全管理策略,

要完全、彻底、安全地清除和覆盖,使其无法被恢复重用;对含有敏感信息的重要设备或存储媒体,需要选择有资质的机构进行安全销毁,并保留处理记录。

互联网电子政务系统在需要迁移前,数据按需进行备份,转移时按业务迁移规范,实现政务业务安全平稳的迁移,支持政务业务的可用性、稳定性和持续性要求。

6 技术体系

6.1 概述

为保障依托互联网基础设施构建的互联网电子政务网络安全,按 GB/T 22239 构建互联网电子政务网络安全技术体系,见图 2。

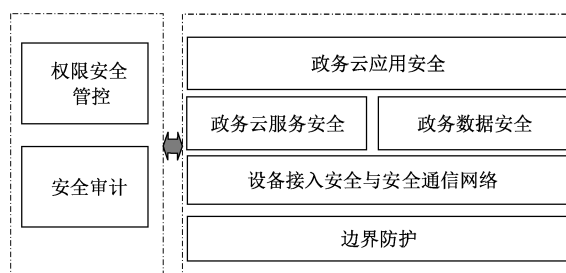


图 2 互联网电子政务网络安全技术体系

6.2 边界防护

边界防护包括如下内容：

- 宜具有基于策略的网络访问控制功能,根据政务应用服务的范围进行网络级访问控制,阻断来自互联网的安全威胁;
- 在基于云计算环境部署虚拟网络及设备的情况下,宜部署虚拟防火墙,对政务云内部多租户之间实现隔离与控制;宜基于容器隔离规则对政务服务实施隔离,实现业务资源虚拟化条件下的东西向数据流向控制,见 GB/T 31168;
- 宜进行网络入侵防范,具有对典型 SYN Flood、DDoS、webshell 等恶意行为进行实时监控、告警和溯源功能,既支持对传统政务服务部署架构的入侵防范能力,又支持对政务虚拟化云环境进行入侵防范的能力;
- 宜在互联网政务服务区和公共政务业务区之间进行可信可靠的隔离与交换,防止来自互联网政务服务区的风险扩散至公共政务业务区。

6.3 设备接入安全与安全通信网络

设备接入安全与安全通信网络包括如下内容：

- 在用户设备接入时宜进行设备接入保护,具体接入要求见 GB/T 31168;
- 依托互联网基础设施,宜采用密码技术、安全策略管理、安全隧道管理、安全审计管理和动态评估等技术,宜采用 IPSec 或 SSL 协议,在异地政府机关与政务中心之间、远程政务办公用户与政务中心之间进行安全互联,构建远程用户与政务服务平台之间虚拟化安全通信网络;
- 宜通过用户身份鉴别、虚拟安全域构建、接入终端状态评估、数据加解密和云环境微隔离等技术,实现政务数据传输的安全;
- 宜通过网络设备标识、用户账户管理、网络身份鉴别和网络登录控制等技术,实现网络设备连接的安全;

- e) 宜通过划分子网和网段、网络设备冗余部署和网络带宽性能提升等手段,实现网络架构的安全。

6.4 政务云服务安全

政务云服务安全包括如下内容:

- a) 互联网政务云宜具备恶意代码防护功能,具体要求见 GB/T 31168;
- b) 互联网政务云宜具备虚拟机镜像安全、虚拟化平台的资源隔离和虚拟机安全隔离等功能,具体要求见 GB/T 31168;
- c) 宜具备存储虚拟化安全性要求,实现不同云租户虚拟存储资源的逻辑隔离,具体要求见 GB/T 31168;
- d) 对政务信息和系统资源宜具备访问控制功能,具体要求见 GB/T 31168,宜对云平台上的信息流进行有效的信息流向控制,防止不同域之间以违背信息流策略的方式进行流动,具体要求见 GB/T 31168;
- e) 宜具备 API 访问安全功能,防止 API 被恶意利用,具体要求见 GB/T 31168。

6.5 政务数据安全

政务数据安全包括如下内容:

- a) 宜对重要政务数据文件、结构化与非结构化数据进行加密存储,加密存储方式见 GB/T 35274;
- b) 宜对政务应用中产生的大数据,采用基于角色的访问控制机制、基于属性的访问控制机制等对互联网政务大数据进行灵活授权、分类防护和动态控制;
- c) 对于互联网电子政务应用中处理的个人敏感信息,按 GB/T 35273 要求,对银行账户、财产、征信和健康生理等个人敏感信息提供安全保护。

6.6 政务云应用安全

政务云应用安全包括如下内容。

- a) 宜将互联网政务服务、互联网政务办公的应用与数据进行分区存储,存储方式见 GB/T 37973。
- b) 对政务云中不同的系统与服务,宜进行信息分类防护。对互联网政务服务云业务,宜重点防护系统和信息的完整性和可用性;对互联网政务办公云业务,宜重点实现政务人员身份鉴别、政务资源授权访问、数据存储安全和信息传输保护等。
- c) 对互联网政务应用区的政务云,宜采用访问控制手段作为对外的统一接入点对外来访问请求进行过滤和转发。

6.7 权限安全管控

权限安全管控包括如下内容:

- a) 宜依托 PKI 向政务用户颁发数字证书,进行政务用户身份鉴别;
- b) 宜对政务办公与政务服务等业务进行权限管理,提供信任的建立、保持、维护和管理等功能;
- c) 权限管理宜包括身份标识、身份鉴别、授权管理和访问控制等内容,支撑互联网政务系统级、任务级、数据级的安全管控,减少系统攻击面;
- d) 宜基于访问人员的身份标识、角色及属性对政务访问行为进行多样化访问控制;
- e) 权限管理中的访问主、客体宜具有唯一身份标识,在访问行为发生过程中宜持续进行信任评估与访问控制。

6.8 安全审计

安全审计包括如下内容:

- a) 宜对互联网电子政务系统中的安全行为、安全事件进行安全审计,支持行为溯源与责任认定;
- b) 宜对汇聚的安全数据和行为进行智能分析,对未知新型攻击等威胁源进行分析检测,对政务服务网络遭受攻击的事件进行分析,对可能出现的安全事件进行预警,根据安全事件进行安全设备与安全策略的动态调整。

7 体系实施原则

7.1 按需保护原则

在基于互联网的电子政务建设中,根据安全需求,合理配置网络安全资源,采取适当的安全措施,进行有效的安全管理,从管理、技术等各个方面进行综合防范。

7.2 权限最小化原则

对政务应用的访问权限实施最小化原则。

7.3 系统分域控制原则

对电子政务信息系统的防护根据系统及其数据的重要程度和敏感程度的不同,进行分域存储、分域边界防护和域间访问控制。

7.4 动态防护原则

采用身份鉴别、授权管理、访问控制和动态评估等安全措施,构建从用户、实体到网络、政务资源的动态安全防护架构。

7.5 残余信息保护原则

对基于互联网电子政务系统中敏感资源的任何残余信息内容,在资源分配或释放时,需实现用户鉴别信息所在存储空间的完全清除,需实现系统内的文件、目录和数据库记录等资源所在存储空间的完全清除。

7.6 供应链安全原则

政务平台建设所涉及的服务器、终端、固件、软件和显卡,以及政务网站、政务 App 中使用的开源框架和开源软件等,需采用安全可信的软硬件产品,具体要求见 GB/T 43698 和 GB/T 36637。

8 体系实施框架

8.1 传统业务部署模式下的体系实施框架

8.1.1 基本结构

在互联网电子政务系统建设中,相关地市级政府部门根据应用的需要,采用传统硬件服务器部署模式进行数据存储与应用系统建设,即传统业务部署模式。在该模式下,县区/乡镇等行政办公区域通过互联网进行数据共享与管理,远程办公用户通过网络方式进行远程数据安全访问,安全体系实施更加关注互联网电子政务应用区及用户侧的网络安全,其实施框架见图 3。

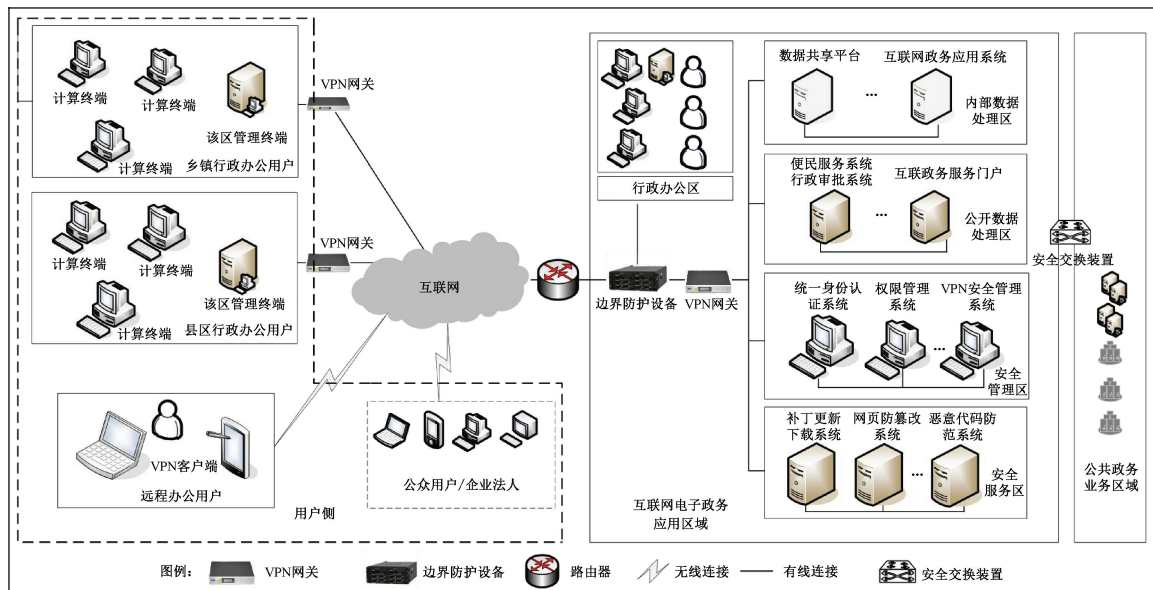


图3 传统业务部署模式下的体系实施框架

8.1.2 用户侧

用户侧是指依托互联网访问互联网电子政务应用区的用户。包括：公众用户/企业法人、远程办公用户、县区行政办公用户和乡镇行政办公用户。

8.1.3 边界防护设备

边界防护设备通常为高性能防火墙，位于互联网电子政务应用区域的边界，实现基于安全策略的网络接入控制和入侵防范。

8.1.4 VPN 网关

位于边界防护设备之后，与用户侧的VPN网关或VPN客户端一起，共同构建出基于互联网的虚拟化安全政务网络，实现行政远程办公用户的移动安全接入与访问，支持区县/乡镇行政办公用户的安全办公与信息交换。

8.1.5 互联网电子政务应用区域

互联网电子政务应用区域是互联网电子政务应用所涉及的数据存储、数据处理、网络运维、安全管理、安全服务的区域，包括：内部数据处理区、公开数据处理区、安全管理区和安全服务区四个区。内部数据处理区存放互联网电子政务办公平台、数据共享平台等涉及政务办公的数据库服务器与应用服务器。公开数据处理区存放面向社会公众用户/企业法人的互联网政务服务系统、行政审批系统等数据库服务器与应用服务器。安全管理区存放对用户身份、权限、策略等信息进行统一管理的终端或服务器。安全服务区是方便用户进行安全运维的区，存放补丁更新下载、网页防篡改和恶意代码防护等安全服务器。

在互联网政务应用区域，根据政务数据的敏感级别，将内部政务数据和公众公开数据分开存储，通过分域控制设备进行有效的隔离，并采用数据安全交换技术实现不同数据处理区信息间的单向受控交互，支持政务数据的合规使用。

8.1.6 公共政务业务区域

公共政务业务区域与互联网电子政务应用区域进行安全隔离,当需要进行跨域数据共享时通过安全交换装置进行数据共享。

8.2 云计算部署模式下的体系实施框架

8.2.1 基本结构

与传统业务部署模式不同之处在于互联网政务系统的建设与运行依托政务云构建。在云计算部署模式下,地市级政务部门建设政务云与数据中心,或级联上级政务云,并在政务云的基础上分别建设面向政务人员的政务办公应用、面向公众与企业用户的政务服务应用、用于安全管理与运维的安全管理平台 and 用于防恶意代码与补丁更新的安全服务平台。它与下辖的地市垂直管理部门、乡镇行政办公区域、远程办公用户进行安全接入与互联,构建虚拟化安全政务网络,实现远程安全政务办公、数据安全共享和信息上报与汇总。云计算部署模式下的安全体系实施框架见图 4。

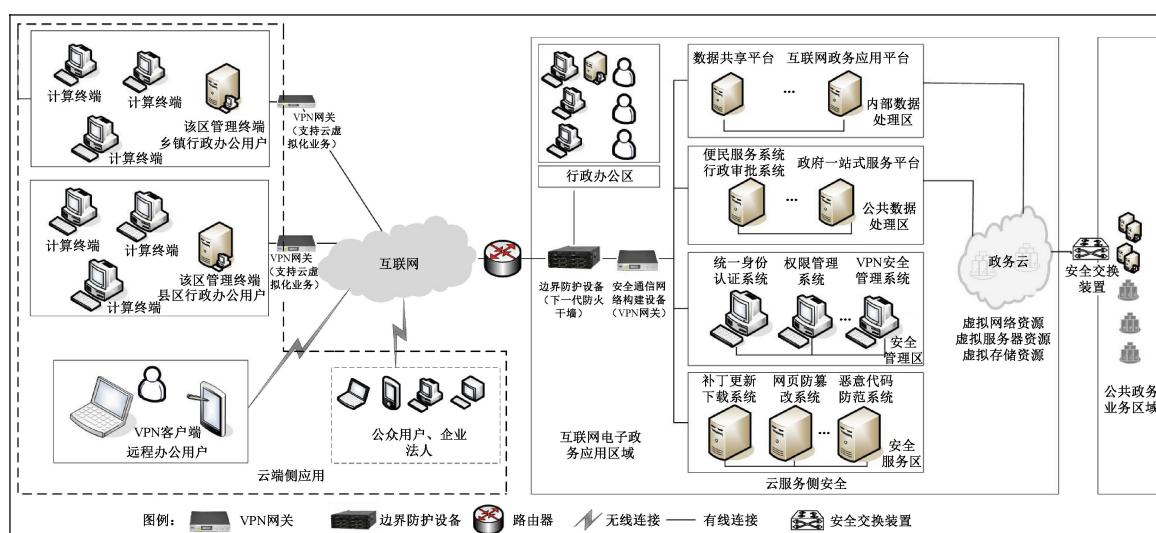


图 4 云计算部署模式下的体系实施框架

8.2.2 政务云

在互联网电子政务应用区域,云计算部署模式包括:公有云、私有云、混合云和云租赁等,在这里统称为政务云。地市级政务部门采用云部署模式时,既可选择通过评估的云服务商,云服务商选择与部署要求见 GB/T 31167,也可租用其他连接互联网的电子政务云平台。

8.2.3 云端侧应用

云端侧应用面向的是公众用户/企业法人、远程办公用户、县区行政办公用户和乡镇行政办公用户,部署于远程办公用户终端的 VPN 客户端需支持虚拟化云桌面,部署于县区/乡镇行政办公区域边界的 VPN 网关需支持云虚拟化业务。

8.2.4 边界防护设备

在云计算部署模式下,边界防护设备通常为下一代防火墙,宜支持云计算部署模式下的虚拟化资源隔离与保护,实现虚拟化网络资源防安全防控,支持云信息流南北向访问安全。

8.2.5 安全通信网络构建设备

在互联网电子政务区域边界,需部署用于安全通信网络构建的设备,即支持云虚拟化业务的 VPN 网关及其 VPN 管理系统,与用户侧的 VPN 客户端(支持虚拟化云桌面)或 VPN 网关,共同构建出基于互联网的虚拟化安全政务网络,实现行政远程办公用户的移动安全接入与访问,支持区县/乡镇行政办公用户的安全办公与信息交换。

8.2.6 云服务侧安全

在云服务侧,在对互联网政务应用分区存储的基础上,宜对用户、租户、角色和资源进行统一管理,实现虚拟化资源、政务大数据的统一权限管理。在用户身份鉴别的基础上,针对虚拟化资源、政务大数据进行动态访问控制,实现安全的互联网政务办公和政务大数据的合规使用。

宜支持地市级(或县区级)政府部门一站式公众服务平台的可信与可靠,对上报与传送的信息进行逐级审核与把关,防止对公共服务平台的攻击与篡改,具有有效的逐级恢复能力。

在政务云内部,宜与信息流防控组件相结合,实现云多租户隔离与控制、云 API 微隔离等功能,支持云信息流东西向访问安全。

9 密码使用与安全保密职责

9.1 密码使用

密码使用包括如下内容:

- a) 互联网政务服务网络需使用国家密码管理主管部门认证核准的密码技术和产品,并按国家密码管理部门与政务行业有关要求使用密码算法,具体要求见 GB/T 37092 和 GB/T 39786;
- b) 政务服务网络需采用 PKI 实现用户和设备的身份标识,为用户身份鉴别、网络设备安全接入提供服务,PKI 建设与运行的具体要求见 GB/T 30272。

9.2 安全保密职责

安全保密职责包括如下内容:

- a) 依据《中华人民共和国保守国家秘密法》第三十一条及《中华人民共和国保守国家秘密法实施条例》第三十四条规定,相关机关、单位需加强保密自监管,开展督促检查;
- b) 相关机关、单位需加强对基于互联网电子政务系统、信息设备的保密管理,及时发现并处置安全保密风险隐患。

参 考 文 献

[1] 《中华人民共和国保守国家秘密法》(1988年9月5日第七届全国人民代表大会常务委员会第三次会议通过,1989年5月1日施行;2010年4月29日修订,2010年10月1日施行;2024年7月1日修订,2024年10月1日施行)

[2] 《中华人民共和国保守国家秘密法实施条例》(国务院令 第646号,2014年1月17日公布,2014年3月1日施行;2024年7月10日修订,国务院令 第786号,2024年9月1日施行)
