ICS 35.040
L 80

中华人民共和国国家标准化指导性技术文件

GB/Z 24294.1—2018
部分代替 GB/Z 24294—2009

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

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

2018-03-15 发布　　2018-10-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB/Z 24294《信息安全技术　基于互联网电子政务信息安全实施指南》分为以下部分：

——第 1 部分：总则；

——第 2 部分：接入控制与安全交换；

——第 3 部分：身份认证与授权管理；

——第 4 部分：终端安全防护。

本部分为 GB/Z 24294 的第 1 部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

本部分部分代替 GB/Z 24294—2009《基于互联网电子政务信息安全实施指南》。与 GB/Z 24294—2009 相比，主要技术变化如下：

——补充了基于互联网电子政务信息安全参考模型；

——对基于互联网电子政务信息安全技术体系做了新修改；

——针对基于互联网电子政务实施架构给出了新的建议；

——针对接入控制与安全交换给出了新的建议；

——针对互联网电子政务移动终端新的应用模式给出了新的建议；

——针对信息分类防护的具体应用做了新补充；

——针对信任体系建设给出了身份认证与授权管理新建议。

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。

本部分由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本部分起草单位：解放军信息工程大学、中国电子技术标准化研究院、北京天融信科技有限公司、郑州信大捷安信息技术股份有限公司。

本部分主要起草人：陈性元、杜学绘、孙奕、曹利峰、张东巍、任志宇、夏春涛、何骏、景鸿理、上官晓丽。

本部分所代替标准的历次版本发布情况为：

——GB/Z 24294—2009。

引　言

互联网已成为重要的信息基础设施，积极利用互联网进行我国电子政务建设，既能提高效率、扩大服务的覆盖面，又能节约资源、降低成本。利用开放的互联网开展电子政务建设，面临着计算机病毒、网络攻击、信息泄漏、身份假冒等安全威胁和风险。为推进互联网在我国电子政务中的应用，指导基于互联网电子政务信息安全保障工作，特制定本指导性技术文件。

基于互联网电子政务信息安全实施指南标准由基于互联网电子政务信息安全实施指南总则、接入控制与安全交换、身份认证与授权管理、终端安全防护四部分组成。基于互联网电子政务信息安全实施指南总则，是基于互联网电子政务信息安全建设的总揽，可指导政府部门建立基于互联网电子政务信息安全系统，构建基于互联网电子政务信息安全技术体系；接入控制与安全交换、身份认证与授权管理与终端安全防护三个规范，分别从互联网电子政务中安全互联与接入控制、政务办公与政务服务安全、政务终端安全防护三个关键实施点，对基于互联网电子信息安全系统建设进行规范。

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

1 范围

GB/Z 24294的本部分给出了基于互联网电子政务信息安全参考模型,构建了基于互联网电子政务信息安全技术体系,并对体系的实施原则、实施框架、实施关键技术与风险评估给出指南性建议。为构建基于互联网电子政务信息安全保障架构、建立基于互联网电子政务信息安全系统提供规范。

本部分适用于没有电子政务外网专线或没有租用通信网络专线条件的组织机构,基于互联网开展不涉及国家秘密的电子政务信息安全建设,为管理人员、工程技术人员、信息安全产品提供者进行信息安全建设提供管理和技术参考。涉及国家秘密,或所存储、处理、传输信息汇聚后可能涉及国家秘密的,按照国家保密规定和标准执行。

2 规范性引用文件

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

GB/T 20984—2007 信息安全技术 信息安全风险评估规范

GB/T 30278—2013 信息安全技术 政务计算机终端核心配置规范

GB/T 31167—2014 信息安全技术 云计算服务安全指南

3 术语和定义

下列术语和定义适用于本文件。

3.1

内部数据处理域 inside data processing domain

仅向政务办公人员开放的政务办公系统及其数据的所在域。

3.2

安全政务网络平台 network platform for securegovernment affairs

通过采用商用密码技术和VPN技术,合理配置不同种类的VPN产品,完全基于互联网,实现地市/县区/乡镇等各党政务部门的安全互联互通,所建成的低成本、可扩展的电子政务网络。

3.3

安全政务办公平台 office platform for secure government affairs

通过数据分域存储、统一身份认证、统一授权管理、信息分类防护等安全技术,与电子政务办公应用系统相结合,在实现电子公文的定稿、签发、盖章、发送、接收、打印和归档等全程电子化的同时,使电子政务办公系统中身份可信、行为可控、系统可管,打造安全可控的互联网电子政务办公平台。

3.4

公开数据处理域 public data processing domain

向公众开放的公共服务系统及其数据的所在域。

3.5

域间信息安全交换　secure inter-domain exchange of information

通过安全交换策略，控制不同类别的信息在内部数据处理域和公开数据处理域之间进行安全、可信、可控的传递和处理，防止来自互联网的安全威胁波及到内部数据处理域，以及内部数据处理域内的信息泄露。

3.6

安全管理区域　security management domain

仅向系统安全管理人员开放的安全管理系统及其数据的所在域。

3.7

安全服务区域　security service domain

为用户提供安全服务的系统及其数据的所在域。

3.8

可信公共服务平台　trusted public service platform

通过数据分域存储、统一身份认证、网页防篡改等安全技术，与政府门户网站、政务服务系统相结合，在实现政务公开、政务服务、公众信息互动等公共服务的同时，使公共服务系统中关键身份可信、发布信息真实、关键操作可审核、系统健壮性强等，打造政府的可信开放服务平台。

4　缩略语

下列缩略语适用于本文件。

IP：互联网协议(Internet Protocol)

PIDDE：安全策略—识别—设计—实施—评估(Policy-Identify-Design-Do-Evaluate)

PKI：公钥基础设施(Public Key Infrastructure)

VPN：虚拟专用网(Virtual Private Network)

5　基于互联网电子政务信息安全参考模型

5.1　安全参考模型

安全参考模型用于规范基于互联网电子政务系统的建设流程。组织根据基于互联网电子政务信息安全要求与期望，遵循由“安全策略(Policy)—识别(Identify)—设计(Design)—实施(Do)—评估(Evaluate)”组成的基于互联网电子政务信息安全参考模型(PIDDE)，建立受控的基于互联网电子政务信息安全系统。PIDDE 模型示意图如图 1 所示。

模型描述了组织如何把相关方的信息安全要求和期望作为输入，并通过必要的行动和过程，建立满足这些要求和期望的受控的基于互联网电子政务信息安全系统。通过识别、设计、实施、评估与安全策略的相互作用，给出了基于互联网电子政务信息安全实施过程间的联系。

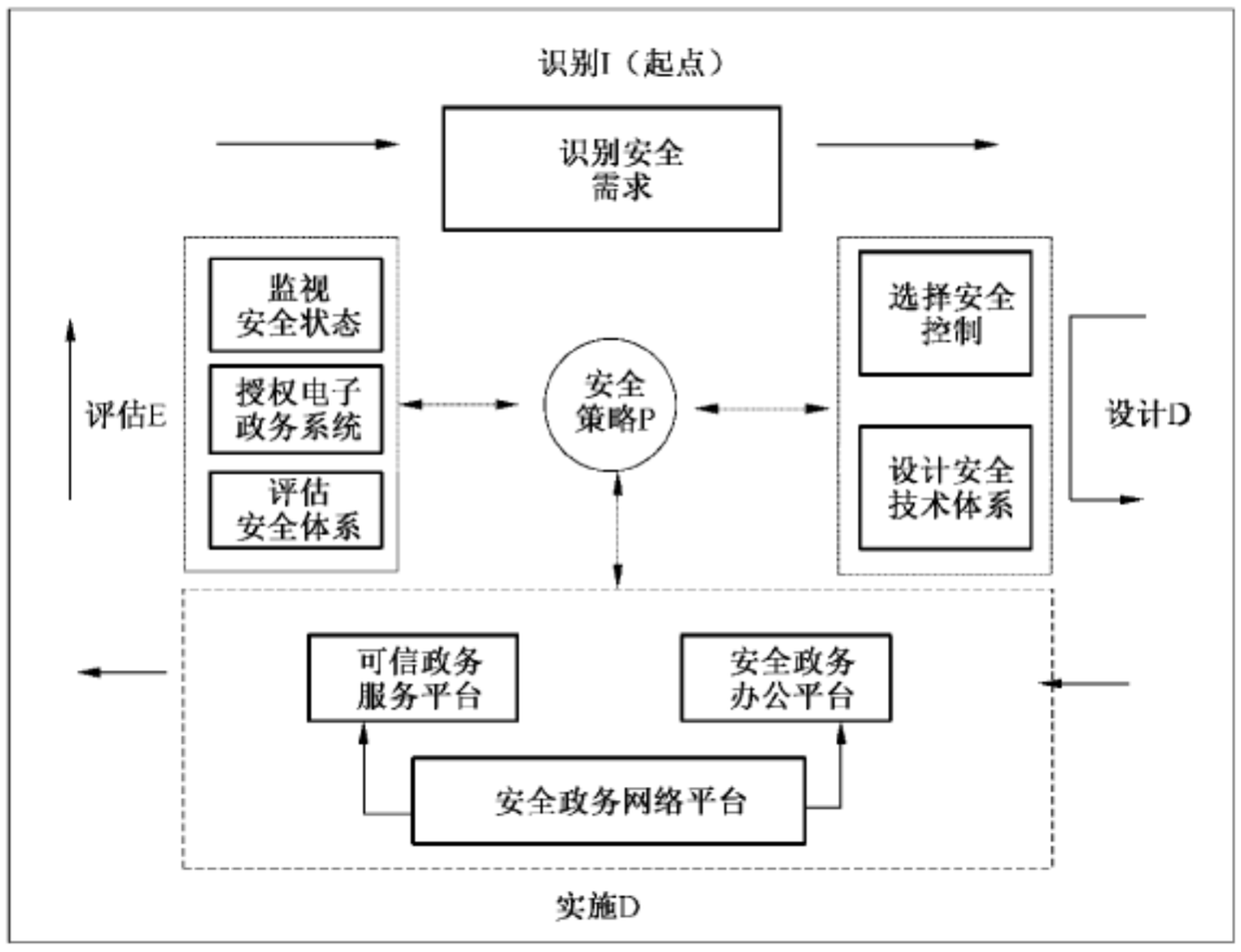

图 1　基于互联网电子政务信息安全参考模型(PIDDE)

5.2　安全策略

5.2.1　安全策略类型

安全策略是用于所有与安全相关活动的一套规则，是规范基于互联网电子政务信息安全技术体系设计、指导信息安全系统建设、进行信息安全动态防御的主要依据，在 PIDDE 模型中处于核心地位，应能够根据系统所面临的风险与需求进行动态调整与变化，以适应不断变化的信息安全形势。基于互联网电子政务信息安全策略自上而下包括：管理类策略与实例类策略两类。

5.2.2　管理类策略

管理类策略主要包括分类防护、分域控制、信任体系构建、终端安全防护、残余信息保护五个策略，用于指导基于互联网电子政务信息安全建设，具体如下：

a)　分类防护策略。根据信息的类别及其重要程度，宜采取不同的保护措施；

b)　分域控制策略。根据系统和数据的重要程度，宜采用系统分域存储、接入控制和域间安全交换等安全措施，实施分域控制；

c)　信任体系构建策略。宜采用身份认证、授权管理、访问控制、责任认定等安全措施，建立一体化互联网电子政务安全信任体系；

d)　终端安全防护策略。对互联网上的电子政务终端，宜根据不同的应用环境，采用不同的终端安全防护模式；

e)　残余信息保护策略。确保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对于所有客体都是不可再利用的。应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。

5.2.3　面向实体的实例类策略

实例类策略是面向安全互联设备、接入控制设备、安全交换设备、终端安全防护设备、认证授权设备的安全规则，是各种安全设备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，应根据

系统中所发生的入侵事件、入侵行为、系统风险，调整信息安全设备中基于规则的信息安全策略。

5.3 识别安全需求

5.3.1 安全需求识别

通过对基于互联网电子政务系统中所包含的应用系统与政务信息的识别，明确基于互联网电子政务系统的安全重点与安全需求。

5.3.2 政务系统识别

通过基于互联网电子政务应用系统识别，明确基于互联网电子政务信息安全所保护的对象及其重要程度，给出不同系统的安全需求，为系统的分类防护、分域存储、分域控制奠定基础。政务系统包括两大类，具体如下：

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、公文交换、公文处理、办公管理和数据共享等。安全防护的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) 公共服务。面向社会公众提供信息公开、在线办事、互动交流等服务。安全防护的重点应放在系统和信息的完整性和可用性方面，特别要防范对数据的非法修改。

5.3.3 政务信息识别

按照 GB/T 31167—2014 规定，基于互联网电子政务系统中的信息分为公开信息和敏感信息两类，具体如下：

a) 公开信息。分为内部公开与外部公开两类。内部公开信息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，外部公开信息是在互联网上可以向公众开放的政务信息；

b) 敏感信息。敏感信息是只有授权的政务人员才能访问的信息，主要包括政府单位不宜公开的工作信息、企业的商业秘密、个人隐私等。

5.4 安全设计

5.4.1 选择安全控制

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，以及所采用的应用技术，选择合适的安全技术与安全控制项，构建不同的基于互联网电子政务信息安全实施架构，具体的安全控制项参见附录 A。

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，宜依托公钥基础设施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，实现安全互联、接入控制与边界防护、区域安全、终端安全、应用安全、安全服务和安全管理，形成一体化的分类分域安全防护体系。

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，宜从政务网络、政务办公、政务服务三个方面，构建安全政务网络平台、安全政务办公平台、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) 安全政务网络平台。采用商用密码、防火墙和 VPN 等技术，依托互联网，通过有线、无线等多

种手段，将各接入单位安全互联起来，形成安全电子政务网络平台。

b) 安全政务办公平台。采用政务人员身份鉴别、政务资源授权访问、政务数据分域控制、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（如政务办公系统、政务审批管理系统等）进行安全保护，形成安全政务办公平台。

c) 可信政务服务平台。采用政务人员身份鉴别、政务信息发布审核、政务服务可靠性保证等安全技术，对政务公众服务系统（如政府门户网站、12345 便民热线、公众信息采集系统等）进行安全保护，形成可信政务服务平台。

5.6 安全评估

5.6.1 评估安全技术体系

在基于互联网电子政务系统建设与运行过程中，采用分析、验证、核查、扫描检测、渗透测试等手段，对系统进行符合性验证与安全风险评估，确保各项安全机制符合基于互联网电子政务信息安全实施要求，降低信息安全风险。

在对基于互联网电子政务系统进行安全评估后，宜给出信息安全评估报告，针对信息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与安全策略调整。

5.6.2 授权电子政务系统运行

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，如果在可授权的范围内，则批准电子政务系统运行，并同时授权组织定期测试和评估信息安全策略、流程及管理、技术和运行措施的有效性。

5.6.3 监视安全状态

通过系统识别、安全监控、监视分析、安全审计等手段，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、对异常行为进行统计和跟踪，识别违反安全策略的行为，使管理员能够有效监管、控制和评估互联网电子政务系统中的安全行为。

6 基于互联网电子政务信息安全技术体系

6.1 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，宜建立安全技术体系，保障电子政务信息的保密性、完整性、可用性、真实性和可控性，保证系统的整体安全性。基于互联网电子政务信息安全技术体系的示意图如图 2 所示。

图 2 基于互联网电子政务信息安全技术体系

互联网是构建电子政务系统的基础设施。依托公钥基础设施，从安全互联与接入控制、边界防护到区域安全、终端安全、应用安全，从安全服务到安全管理，构建基于互联网电子政务信息安全技术体系，

形成安全政务办公平台、可信政务服务平台与安全政务网络平台，保障基于互联网电子政务系统的安全，示例参见附录 B。

6.2 公钥基础设施

公钥基础设施主要是为用户和实体提供数字证书服务，应参照国家的有关规定，选用依法建设的证书服务系统。公钥基础设施采用的 PKI 技术要求能够保证系统的互联互通和将来的功能扩展，满足国家密码管理局发布的有关密码行业标准的相应要求。

6.3 安全互联与接入控制、边界防护

安全互联与接入控制、边界防护主要是实现区域间的安全互联，为各区域提供网络边界防护，为政务办公用户提供移动安全接入。采用的主要安全技术包括商用密码、VPN、防火墙、分域控制等技术，依托互联网，实现市、区县、乡镇三级政府和移动办公用户的安全接入与互联。

6.4 区域安全

区域安全主要是按照“明确责任、各负其责”的原则，相关部门根据安全需求为各区域提供网络安全保障。采用的主要安全技术包括入侵检测、漏洞扫描、安全审计、网页防篡改、防病毒等技术，实现区域所需的安全防护。

6.5 终端安全

终端安全主要是为互联网上的政务办公终端提供恶意代码防范、基于主机的访问控制、传输安全、存储安全、电子邮件安全、安全审计、终端可信性验证等综合安全防护措施。终端安全应用模式包括终端基本安全、终端增强安全和移动终端安全等三种模式，采用的主要安全技术包括系统安全核心配置、防恶意代码、登录认证、访问控制、电子邮件安全、安全公文包等，实现多应用模式下的政务终端安全防护。终端基本安全防护中安全核心配置方法依据 GB/T 30278—2013。

6.6 应用安全

应用安全主要是为电子政务应用系统提供信息分类分域存储、统一身份认证、授权管理、访问控制、责任认定、信息分类防护、域间信息安全交换等安全措施。按照“分类分域防护”策略，采用相应的安全技术实施应用系统及相关信息的安全保护，主要安全技术包括加密技术、数字签名技术、统一身份鉴别技术、授权管理与访问控制技术、信息安全交换技术、基于工作流的访问控制技术和网页防篡改技术等。

6.7 安全管理

安全管理主要是为电子政务系统提供安全设备管理、授权管理、安全策略管理、安全审计、检测评估等措施。采用的主要安全技术包括授权管理技术、VPN 安全管理技术、审计管理技术、应急处理技术、漏洞扫描技术等。安全管理面向的是 VPN、入侵检测、安全审计等安全设备或系统，是这些设备安全、正确运行的保证。

6.8 安全服务

安全服务主要是为各类用户提供单点登录、系统补丁下载、终端安全配置模板分发、恶意代码库升级等在线服务。采用的主要安全技术为统一身份鉴别、恶意代码防范等。安全服务面向的是电子政务系统中的最终用户，为最终用户进行身份认证、系统升级提供便利。

7 体系的实施原则

7.1 按需保护原则

基于互联网的电子政务建设应根据应用系统的安全需求，合理配置信息安全资源，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

对政务信息系统应用及其信息的访问权限应实施最小化原则，非工作必需知悉的人员，不得具有有关系统及信息的访问权限。

7.3 信息分类防护原则

电子政务系统的防护措施应面向它所处理的信息，根据不同类别的信息采取不同的保护措施。

7.4 系统分域控制原则

对电子政务信息系统的防护应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，保证信息的安全隔离和安全交换。

8 体系的实施架构

8.1 数据集中模式下的体系实施架构

8.1.1 基本结构

在互联网电子政务系统建设中，一些地市级政府部门根据应用的需要将数据进行集中存储、集中管理，即数据集中模式，包括传统数据存储与新型云计算模式。此模式下市/县/乡的数据既要实现物理上集中存储，又要实现逻辑上的隔离，数据大集中模式下的安全体系实施架构的示意图如图 3 所示。

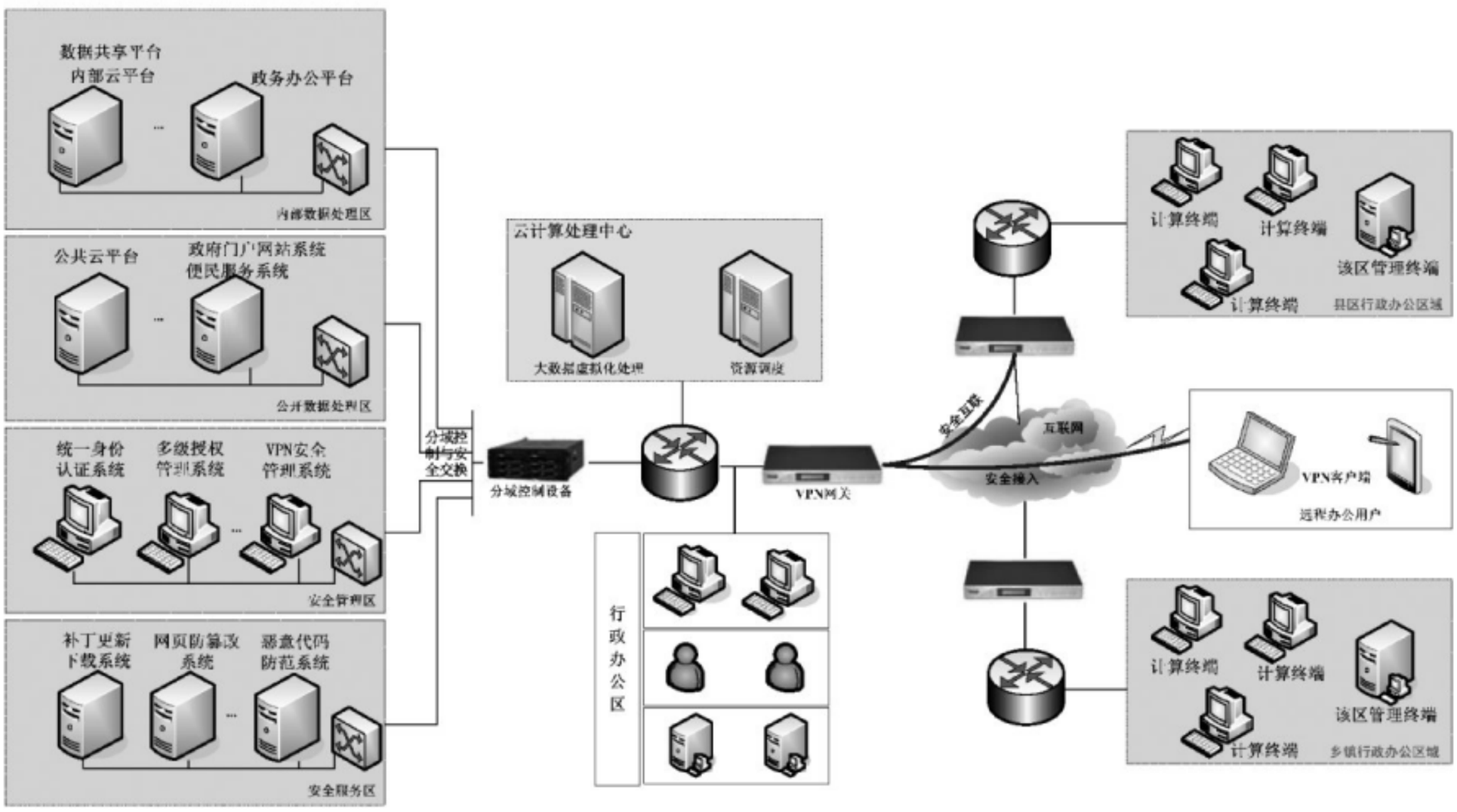

图 3 数据集中模式下的安全体系实施架构

在数据集中/云存储模式下，地市/县区/乡镇组建集中化的数据中心，为用户提供透明化的虚拟服务，实现资源共享。县区与乡镇行政办公区域通过互联网进行数据共享与管理，远程办公用户通过移动互联方式进行远程数据安全访问。根据政务系统与数据的敏感级别，通过分域控制网关进行有效的隔离，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。在此模式下，应通过有效的

权限划分实现各部门间的信息隔离，具备与原有行政体制相适应的逻辑流程。

若采用云计算模式，在内部数据处理域宜构建内部云平台，在公开数据处理域宜构建公共云平台，具体构建方法依据 GB/T 31167—2014。

8.1.2 安全政务网络平台

在地市数据中心配置高性能中心 VPN 网关，在县区行政办公区域与乡镇行政办公区域配置普通 VPN 网关，远程办公用户配置 VPN 客户端，既实现部门间的安全互联，又实现移动安全办公，保证政务办公信息在互联网上的安全保密传输，构建可扩展的统一安全政务网络平台。

在安全政务网络平台构建时，宜支持统一的 VPN 安全策略管理，既支持各类政务应用的安全透明应用，又支持手机、掌上电脑(PDA)、笔记本等多类型终端的 WEB(用于仅通过浏览器就能访问的应用程序)应用与 WAP 应用(使用网页技术在手机等移动终端展示的应用程序)。

8.1.3 面向逻辑多级的安全政务办公平台

8.1.3.1 多级授权管理

地市/县区/乡镇分级分部门进行权限管理是安全政务平台的管理要求。为实现面向逻辑多级的安全政务办公平台的构建，需要进行多级授权管理。政务应用系统和安全管理系统部署在地市数据中心，实现分级分部门权限分隔与管理；地市/县区/乡镇各部门配置本区域管理终端，实现用户管理、角色管理、资源管理、权限分配、统一安全审核与责任认定。多级授权管理内容如下：

a) 分级部署。支持授权管理系统内部的分级管理，构建虚拟授权树，通过为管理员划分管理范围，实现逻辑分级，满足不同管理单位、不同安全级别的权限管理需求；

b) 用户管理。在地市/县区/乡镇本区域管理终端上，通过统一身份认证与授权管理系统，选择所在组织部门，采用统一的用户身份信息规范标准，按照统一的编码方案，设置本区域用户与角色编码表，并将其逐级上传至管理平台；

c) 统一资源管理。在地市区域管理终端上，通过统一身份认证与授权管理系统，对全市政务应用平台的网络资源、信息资源、应用资源进行统一管理，为权限管理作好准备；

d) 多级权限分配。在地市/县区/乡镇本区域管理终端上，通过统一身份认证与授权管理系统，根据用户的岗位与角色，按照最小权限原则，对各部门的资源进行权限分配；

e) 统一安全审计与责任认定。在地市区域的认证授权管理平台上，应实时记录用户的操作行为，形成政务应用操作日志，方便事后追踪与责任认定。

8.1.3.2 政务流程逻辑构建

根据全市组织部门的行政隶属关系，按照行政办公流程，对政务办公系统的政务流程进行统一规划与构建，在各地市/县区/乡镇数据集中管理模式下，实现各地市/县区/乡镇部门的逻辑隔离，并构建与原有行政隶属关系相匹配的政务办公流程。

8.1.4 可信公共服务平台

在该模式下，应充分利用数字证书、统一身份认证等手段，将各县市/乡镇的服务信息进行审核、发布与收集，保证信息发布与收集的真实与可信。

8.2 数据分布存储模式下的体系实施架构

8.2.1 基本结构

在互联网电子政务系统建设中，依据应用需求，有些地市级政府部门仍有部分数据分散存储在县区

信息中心，即数据分布存储模式。数据分布存储模式下，由于地市/县区/乡镇的数据进行了物理隔离，因此，为实现数据安全共享，宜进行安全的信息汇总与信息传输。数据分布存储模式下互联网电子政务安全体系实施架构的示意如图 4 所示。

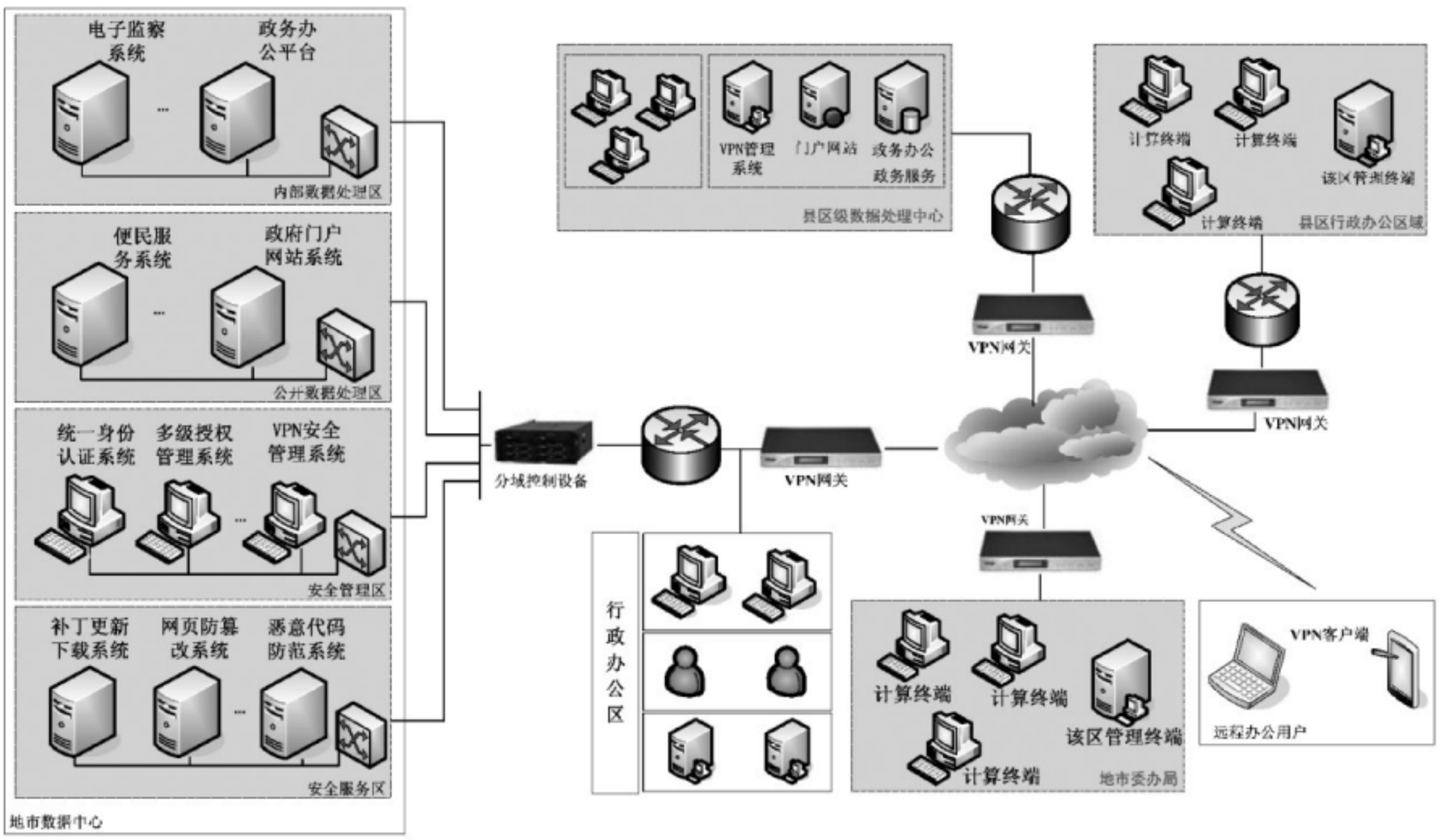

图 4　数据分布存储模式下的安全体系实施架构

在数据分布存储模式下，地市与县区分别建设数据中心，实现数据的物理隔离。根据系统与信息的敏感程度与安全功能的不同，地市数据中心将安全域划分为内部数据处理域、公开数据处理域、安全管理区、安全服务区四区域，进行系统部署与数据存储，它与下辖的地市委办局进行安全互联，实现地市级安全政务办公。较大的县区级单位可以设立自己的数据中心，其安全域划分参考地市级数据中心安全域的划分方式，它与下辖的乡镇行政办公区域进行安全互联，实现县区级安全政务办公。县区级数据中心与地市级数据中心通过 VPN 网关进行安全互联，配置安全交换节点，安全实时地将政务数据进行汇总与处理，实现信息安全交换与共享。

8.2.2　分层分级安全政务网络平台

8.2.2.1　安全政务网络平台

在互联网电子政务数据分布存储模式下，通过 VPN 设备与 VPN 管理系统，基于互联网构建出地市级安全政务网络平台、县区级安全政务网络平台，同时支持本层本级远程用户的移动安全接入与访问，支持跨层跨级用户的移动安全接入与访问，最终构建出能够进行安全互联互通的分层分级安全政务网络平台。

8.2.2.2　VPN 分层分级管理

保护地市级数据中心的高性能 VPN 网关与地市委办局的普通 VPN 网关进行安全互联，应实施地市级统一的 VPN 安全管理，包括地市级 VPN 用户与设备可视化管理、VPN 隧道管理、安全关联管理与协商、安全策略管理、安全审计等内容。

保护县区级数据中心的县区级 VPN 网关与下辖乡镇级 VPN 网关进行安全互联，应实施县区级统

一的 VPN 安全管理，包括县区级 VPN 用户与设备可视化管理、VPN 隧道管理、安全关联管理与协商、安全策略管理、安全审计等内容。

8.2.2.3 地市级与县区级 VPN 安全隧道构建

为实现县区级与地市级数据安全汇总与上报，应在地市级高性能 VPN 网关与县区级 VPN 网关之间构建安全隧道，支持下级 VPN 隧道与上级 VPN 隧道的安全级联。各层各级 VPN 设备应能够进行互联互通，具有层间安全策略配置、安全隧道构建等功能。

8.2.2.4 跨层跨级 VPN 访问管理

由于分布式数据存储模式中 VPN 设备采用分层管理方式，在 VPN 动态拓扑关系构建方面，既要支持本级用户的移动安全接入与安全政务办公，又要支持跨级用户的移动安全接入、跨级跨域 VPN 设备的安全互联，构建动态可扩展的 VPN 拓扑关系，使跨层跨级安全访问成为可能。

8.2.3 安全政务办公平台

8.2.3.1 跨层跨级权限管理

在数据分布存储模式下，对用户、资源、角色、权限管理宜分层分级完成，应采用数字证书实现分层分级的身份认证，构建地市级政务流程与县区级政务流程，实现分层分级的安全政务办公。

在政务模式下，应支持跨层跨级用户的身份认证与安全访问。通过基于数字证书的统一身份认证与授权管理系统，实现跨层跨级用户与角色的映射、跨层跨级权限管理，达到跨层跨级身份认证与跨层跨级用户访问的目标。

8.2.3.2 安全信息交换与共享

地市级数据中心需要向县区级数据中心推送政务信息，县区级数据中心需要向地市数据中心上报基层数据，地市级数据中心与县区级数据中心之间存在着信息安全共享需求。为确保两级部门数据进行安全的信息共享，必须确保数据能够进行受控安全交换，具体如下：

a) 文件级受控交换——如果两级政府部门之间需要共享的数据是文件，宜选用面向文件的安全交换方式，通过定制所交换文件的类型、目录、粒度，实现文件级信息安全共享；
b) 数据库级受控交换——如果两级政府部门之间需要共享的数据是数据库，宜选用面向数据库的安全交换方式，通过定制所交换数据库的表单、字段，实现数据库级信息安全共享；
c) 选择交换模式——根据交换与共享任务的需要，选择点对点交换模式或订阅/发布交换模式。当只存在上级政府部门与少数下级部门信息安全共享需求时，宜采用点对点交换模式；当存在上级政府部门与多个下级部门信息安全共享需求时，宜采用订阅/发布模式；
d) 定制交换策略——定制交换信息的流向、交换任务名称、交换任务类型、交换任务内容等交换策略，保证两级政府部门受控、单向、安全的信息交换；
e) 启动专用交换进程——在两级数据中心交换节点间配置安全交换节点，启动专用交换进程，启动交换任务，进行信息安全交换，防范恶意进程对共享信息的窃取与攻击；
f) 交换过程监管——对交换内容进行提取、转换与过滤、交换进程行为进行评估、交换内容进行审计与追踪，实现两级政府部门交换行为的可管可控。

8.2.4 可信公共服务平台

在该模式下，应保证两级政府部门公共服务平台的可信性与可靠性，对上报与传送的信息进行逐级审核与把关，逐级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。

8.3 移动办公模式下的体系实施架构

8.3.1 基本结构

在互联网电子政务系统建设中，互联网的可伸缩性为随时随地的移动安全办公提供了条件。随着办公系统的深化应用，采用有线无线等多种通信手段，PC 机、笔记本、智能终端等多种信息处理平台，实现无线移动安全办公和贴近式公众服务，即移动办公模式。在移动办公模式下，政务办公系统仍然存放在内部数据中心，在安全结构设计中，一方面应保证政务办公系统能够安全延伸到各种移动终端，另一方面应保证行政办公区域的其他办公终端能够安全访问原有的内部政务办公系统。移动办公模式下的互联网电子政务信息安全体系实施架构的示意图如图 5 所示。

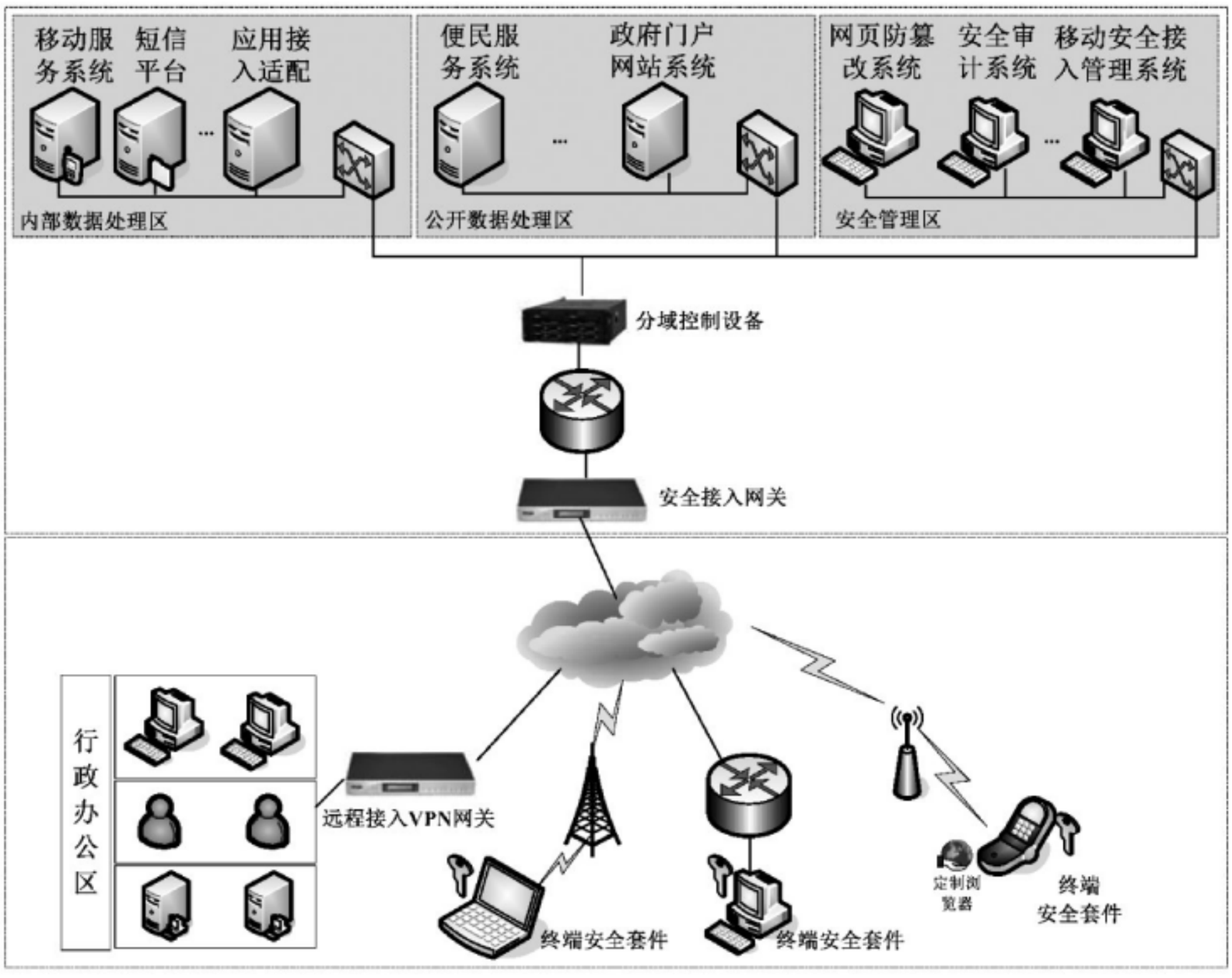

图 5 移动办公模式下的安全体系实施架构

在互联网电子政务移动安全办公模式下，数据中心的应用系统仍然划分为内部数据处理域、公开数据处理域、安全管理区等，为支持无线终端安全接入，内部数据处理域应包括移动服务系统、短信平台、应用接入适配、无线终端接入适配等功能模块，公开数据处理域应包括对外服务系统、政府门户网站系统等，安全管理区应包括网页防篡改系统、安全审计系统与移动安全接入管理系统等。通过配置移动电子政务安全接入网关、无线移动终端安全套件、移动安全接入管理系统，实现基于互联网的消息传输安全、终端安全认证、接入安全审计等，保证多类型终端安全接入内部网络，开展移动安全办公。

8.3.2 无线移动终端安全

8.3.2.1 办公页面解析与展现

无线移动终端（以手持终端为例）宜根据客户端的具体配置（包括移动终端屏幕大小、终端色彩度、终端应用配置等）进行相应的数据解析。

8.3.2.2 无线移动终端参数管理与适配

对不同无线移动终端(以手持终端为例)定制浏览器的相关参数进行配置与管理,并能根据终端参数进行本地适配。

8.3.2.3 数据加解密

无线移动终端从接入内网获取的移动办公数据在互联网传输时应实施信息加密,加解密算法应符合国家商用密码的相关规定,加解密算法应能与终端定制浏览器有效融合。

8.3.2.4 数据解压缩

为提高移动办公数据的访问效率,宜采用适用于无线终端的轻量级解压缩技术,将服务器发送的压缩后数据流在本地进行高速的解压。

8.3.2.5 移动设备本身的安全性

移动设备本身应具有自身安全性,应能够抵御面向移动设备本身的身份假冒、信息窃取、重放攻击等威胁。

8.3.3 无线终端安全适配与接入访问控制

8.3.3.1 数据压缩

移动办公数据在终端安全适配模块发送给定制浏览器之前,应先进行数据流的压缩操作,应用浏览器在终端接收到数据流后,也会进行对应的数据解压操作,从而降低数据访问量,提高数据的访问效率。

8.3.3.2 数据加解密

终端安全适配模块的数据加解密操作宜与其定制浏览器相适应,保证在互联网上传输的办公数据安全。

8.3.3.3 数据预处理与解析

无线终端安全适配模块帮助定制浏览器,将一些对 CPU、内存资源要求较高的操作和运算,以及难以在终端本地进行的 HTML 页面处理操作,在服务器端进行预处理,将处理好的页面内容发送到定制浏览器进行本地的解析与展现。

8.3.3.4 接入用户认证

为确保接入的安全,可针对定制浏览器的来源 IP、终端号码进行认证和鉴权,可根据用户登录的用户名、密码进行接入用户身份认证,也可根据用户所持有的数字证书进行强认证。

8.3.3.5 接入用户访问控制

在移动终端接入认证的基础上,应对终端接入用户进行基于策略的访问控制,防止未授权用户的非法访问。

8.3.3.6 办公应用接入适配与过滤

应用接入适配模块根据相应的过滤规则,将应用页面中不需要在终端上展现的数据进行过滤处理。过滤的对象既可包括广告、页尾等常规部分,也可以是页面中的任意一部分内容。

8.3.4 移动终端安全管理

宜对移动终端用户和策略进行统一的安全管理与配置，对移动终端的访问日志进行统一的审计管理，保证移动终端的可管可控可追责。

9 体系实施的关键环节

9.1 系统分域防控

按照电子政务应用系统信息和应用分类的安全需求，划分为内部数据处理域和公开数据处理域；根据安全系统的功能不同，划分为安全管理区域和安全服务区域。基于互联网电子政务安全域划分的示意图如图 6 所示。具体区域划分与功能如下：

a) 公开数据处理域。公开数据是提供给公众访问的数据。公开数据处理域用来承载处理公开信息的电子政务应用系统及其数据库，或通过云计算方式存储的公开数据，处理对公众和企业开放的服务，如政策发布、政府网站或便民服务等；

b) 内部数据处理域。内部数据是仅允许系统内部人员访问的数据。内部数据处理域用来承载处理内部信息的电子政务应用系统及其数据库，或通过云计算方式存储的内部数据，处理政府内部和部门之间的业务；

c) 安全管理区。安全管理区面向电子政务系统安全管理人员，承载安全管理中心等，为全网的电子政务系统提供统一的身份管理、资源管理、权限管理、策略管理、审计管理和安全可视化管理等；

d) 安全服务区。安全服务区作为安全管理中心的一部分，为所有的电子政务系统用户，提供共性安全支撑服务，如统一身份认证服务、访问控制服务、恶意代码特征库升级、终端安全配置分发等；

e) 在安全域划分的基础上，应实现基于安全策略的分域边界防护、用户安全接入、域间信息安全交换等功能。

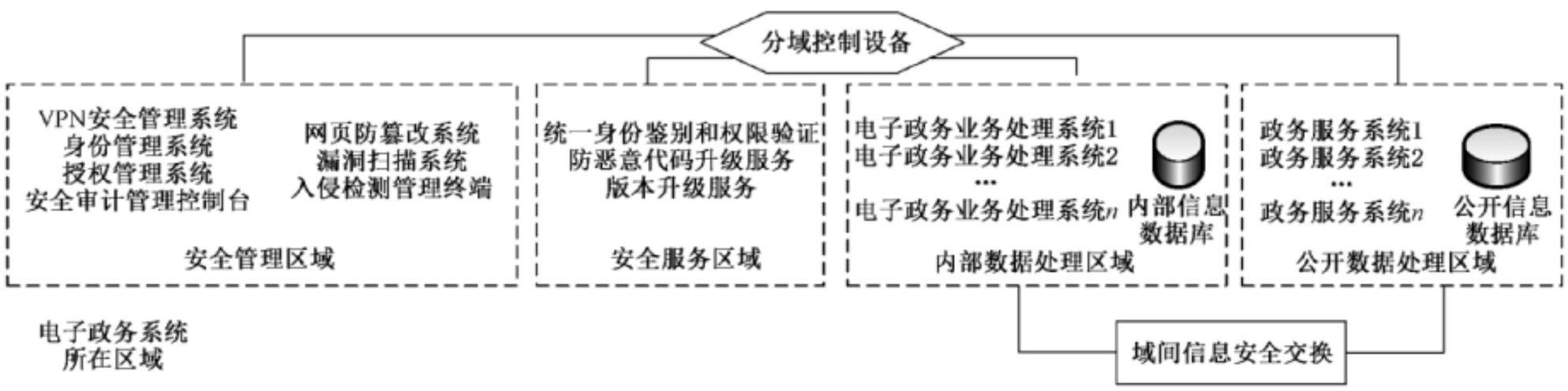

图 6 基于互联网电子政务安全域划分

9.2 统一认证授权

9.2.1 统一身份认证

身份认证是基于互联网电子政务信息系统安全运行的基础。应针对电子政务信息系统身份认证需求，采用高效、安全的一体化身份认证机制，实现用户登录、票据传递与验证、信息系统访问的快速、安全交互，实现一次登录就可以访问多个信息系统的单点登录功能；应能够与电子政务业务系统有效集成，实现登录控制透明化、系统集成集约化。

9.2.2 统一授权管理

基于互联网电子政务信息系统中，为实现电子政务环境下身份可信、资源可管、权限可控，应支持多域多级动态的授权管理。应支持对用户、角色、权限等管理对象进行有效组织，支持基于角色与属性的授权管理，支持对应用资源的权限裁决与细粒度访问控制。

9.3 接入控制与安全交换

9.3.1 接入控制

基于互联网电子政务系统中，应在接入用户进行合法性验证的前提下，依据接入控制策略，针对不同类型的接入用户，实施相应政务资源的授权访问，防止非法用户的非授权访问。

9.3.2 域间信息安全交换

为了实现内部数据处理域和公开数据处理域之间的安全信息共享，应基于域间信息安全交换策略，实施域间可信、可管、可控的信息安全交换措施，防止来自公开数据处理域的木马夹带攻击和内部数据处理域的信息泄漏。

域间信息安全交换技术应支持定制交换与流交换两种模式，应具有交换数据源可信、交换信息保密、交换信息完整、交换内容检测、交换流过滤及交换流可追踪等功能。

9.4 终端安全防护

大多数政务终端在日常办公时所处的物理环境相对固定，终端处理的信息主要是公开信息，终端处于基本安全应用模式。部分终端在政务办公中需要涉及大量敏感信息，终端处于增强安全应用模式。政务人员在移动环境中需要使用不可信终端进行政务办公时，终端处于移动安全应用模式。

终端基本安全应用模式提供政务办公所需的基本安全防护功能，安全配置依据 GB/T 30278—2013。终端增强安全应用模式除应包含终端基本安全防护功能之外，还应包含安全性评估、安全电子邮件和安全公文包等功能。移动终端安全应用模式应构建独立于宿主机的操作系统环境、具有隔离于宿主机硬盘的安全存储区，以及提供可订制的终端安全办公环境。

10 体系的风险评估

10.1 客户访谈

通过对客户访谈，从技术、管理、策略等角度深层次的了解客户信息资产相关的安全要素，分析信息资产背后的风险和潜在的威胁。

10.2 文档信息核查

通过对客户信息资产相关的管理制度、规范、技术文档等的研究和剖析，从更高的层次上发现客户系统中存在的逻辑上的弱点、威胁和风险。

10.3 建设方案分析

通过对基于互联网电子政务信息安全总体建设方案进行深入分析，从安全互联、接入控制与边界防护、区域安全、终端安全、应用安全、安全服务和安全管理等方面进行合理性分析，从方案层面挖掘基于互联网电子政务系统设计上的安全不足。

10.4 方案实施情况核查

通过查看应用系统、主机、服务器等安全配置，查看防火墙、VPN 密码机的策略配置，查看网络部署情况，查看机房物理环境，查看应用系统的分域部署情况等，核查系统建设过程中是否完全遵循总体建设方案和相关技术要求。

10.5 工具检测

通过利用相关扫描和攻击测试工具，对系统的脆弱性和抗攻击能力进行检测，检测系统存在的安全漏洞和威胁。

10.6 评估结论

宜从网络建设、物理环境、网络、主机、电子政务应用系统、安全管理、工具检测等方面分别给出评估的基本结论、存在的问题和整改建议，并汇总形成总体评估的基本结论。评估的具体过程依据 GB/T 20984—2007。

附　录　A
（资料性附录）
某市基于互联网电子政务安全系统配置示例

A.1　VPN 系统

VPN 系统提供网络访问控制、无连接的完整性、数据源认证、机密性、有限的数据流机密性以及防重放攻击等安全服务，具有实体身份认证、域间接入控制、动态组网等功能，并可综合防火墙等安全机制，实现移动安全接入与区域安全互联。VPN 系统通常由 VPN 安全设备、VPN 客户端和 VPN 安全管理设备等三个组件组成，其中，VPN 安全设备是区域间安全互联的必选配置。

VPN 安全设备通常部署于政务网络与外部网络的交界处，进出政务网络的数据流必须经过 VPN 安全设备。VPN 客户端通常安装在移动用户终端上，用于移动用户依托互联网安全地接入政务网络。VPN 安全管理设备部署于安全管理区域，对政务网络中的所有 VPN 安全设备进行管理，包括系统管理、网络管理、安全策略管理、安全隧道管理以及安全审计管理等。

VPN 系统的部署主要分为网络安全互联和移动安全接入两种模式，具体如下：

a）　网络安全互联模式。需要接入互联网电子政务系统的委办局网络，可在委办局网络与互联网的连接处部署 VPN 安全设备，通过建立连接间的安全通道，构建电子政务虚拟专用网络，实现网络安全互联；

b）　移动安全接入模式。政务用户需通过互联网远程访问政务系统时，可在移动办公终端上安装 VPN 客户端，与 VPN 安全设备建立安全通道，实现移动政务办公。

A.2　统一身份认证与授权管理系统

统一身份认证与授权管理系统完成统一的身份管理、身份认证、授权管理等功能。身份管理负责对用户的身份进行统一标识与管理；身份认证负责实现对用户身份的统一鉴别与验证，确保用户身份的合法性；授权管理负责对资源的操作权限进行标识与管理，并为用户授予访问资源的权限，为实现访问控制服务提供支撑。统一身份认证与授权管理系统是基于互联网电子政务系统的必选配置。

统一身份认证与授权管理系统作为安全管理中心的一部分，部署于安全管理区域。

A.3　域间信息安全交换系统

域间信息安全交换系统依据交换任务，基于域间信息安全交换策略，完成内部数据处理域和公开数据域之间信息的适配、提取、转换、过滤、传输、加载等功能，实现可信、可管、可控的域间信息共享与交换。

域间信息安全交换系统主要由主交换节点、从交换节点、交换管理平台三部分组成，部署于内部数据处理区域和公开数据处理域之间。

A.4　终端安全防护系统

终端安全防护系统提供主机恶意代码防范、个人防火墙、桌面存储安全、电子邮件安全、安全审计、系统安全基线配置和可信平台验证等一体化终端安全保护，保护政务终端的安全。用于政务办公的计

算机不应安装与工作无关的软件。

终端安全防护系统适用于三类终端安全应用模式：

a） 终端基本安全应用模式完成系统安全基线配置、主机恶意代码防范、个人防火墙、安全审计等功能；

b） 终端增强安全应用模式是在终端基本安全应用模式的基础上，增加了可信平台评估、存储安全和电子邮件安全等功能；

c） 便携式终端安全应用模式完成以便携式存储设备为载体的自定制操作系统、自定制应用软件和加密存储等功能，用于在不可信的环境下构建安全可信的终端安全计算环境。

A.5 恶意代码防范系统

恶意代码防范系统旨在检测病毒、木马等恶意代码的入侵，并阻止其在电子政务系统中的传播和破坏。

在政务终端、服务器等关键节点上应安装和运行恶意代码防范系统并及时更新恶意代码特征库，定期进行恶意代码扫描和清除。

A.6 网页防篡改系统

网页防篡改系统能够发现网页攻击或篡改，当网页受到破坏时可及时恢复。

网页防篡改系统可与被保护系统部署于同一个区域，通常用于保护通过互联网为用户提供公共服务的系统，如公开数据处理域的政府门户网站。

A.7 安全审计系统

安全审计系统主要用于对基于互联网电子政务系统的安全事件进行跟踪记录和综合梳理。分为网络级审计和系统级审计两种，网络级审计旨在监视和控制来自网络的入侵，记录网络上发生的违规事件。系统级审计旨在对一个系统的运行状况进行记录与评价。

安全审计系统主要由审计数据采集引擎和审计数据分析部件组成。审计数据采集引擎通常部署于被审计的设备中；审计数据分析部件通常部署于安全管理区域。

A.8 入侵检测系统

入侵检测系统通过对网络或主机中的信息进行收集和分析，从中发现违反安全策略的行为和被攻击的迹象。

入侵检测系统包括入侵检测引擎和入侵检测控制台两部分。入侵检测引擎应部署于电子政务系统的重要网络节点和主机节点，入侵检测控制台应部署于安全管理区域。

A.9 漏洞扫描系统

漏洞扫描系统是对网络和主机系统进行扫描、检测，并进行风险管理的工具。用于发现网络和主机系统的安全漏洞，并评估网络和主机系统的安全风险。

漏洞扫描系统应部署于安全管理区域。

A.10 应急响应与备份恢复系统

应急响应与备份恢复系统完成对互联网电子政务系统中突发事件的感知、分析与处理，根据电子政务系统的重要程度进行系统备份与业务持续性保护，保护对象是重要的政务终端和政务系统，实现对政务网络安全运行情况的全方位监测、响应与恢复。

附 录 B
（资料性附录）
某市基于互联网电子政务系统信息分类防护示例

B.1 信息分类方法

B.1.1 信息类别

基于互联网电子政务系统中的政务信息分为敏感信息和公开信息两类，公开信息又分为外部公开信息和内部公开信息。

B.1.2 信息类别的判定

基于互联网电子政务系统中的政务信息分类依据表 B.1 进行判断。

表 B.1 基于互联网电子政务系统信息类别判定表

信息类型		面向用户类型		
		公众	政府工作人员	授权政府工作人员
敏感信息		×	×	√
公开信息	外部公开信息	√	√	√
	内部公开信息	×	√	√
注：“√”表示允许访问；“×”表示不允许访问。				

B.1.3 信息分类示例

以下针对基于互联网电子政务系统中的常见信息进行了分类。具体如下：

a） 敏感信息：

——归档公文；

——酝酿过程中的重要政策、决策、政府工作报告；

——敏感主题的会议信息和会议纪要；

——党务工作信息；

——部工作信息；

——纪检工作信息；

——招标过程信息；

——信访信息；

——涉及公共安全、企业秘密、个人隐私的信息；

——领导活动安排。

b） 公开信息：

1） 内部公开信息：

——政务工作信息，如会议、会务、公告、个人代办公文；
——办理公众服务的过程信息，如签批流程、企业信息、个人信息；
——签批过程中的公文；
——各局委办的内部行政信息；
——内部视频和音频资料；
——政务、党务新闻和要情。

2） 外部公开信息：
——行政法规、规章和规范性文件，国民经济和社会发展统计信息，财政预算、决算报告，社会公益事业建设情况等政务公开信息；
——根据政府职能和工作需求，需要公开的其他信息；
——非政府产生的信息，如新闻、视频等。

B.2 信息分类防护的实施

B.2.1 实施环节

信息的安全防护环节有身份认证、传输安全、存储安全、应用安全、安全审计等。其中，存储安全中包括信息分类存储和备份与恢复；应用安全中包括信息发布审核、网页防篡改、授权与访问控制、分域控制、终端安全等。对信息的安全防护通常在上述环节中完成。

B.2.2 信息分类防护的控制项

根据信息分类防护的安全需求，针对不同类型的信息，在不同的实施环节进行不同程度的安全防护。基于互联网电子政务信息分类防护控制项如表 B.2 所示。

表 B.2 基于互联网电子政务信息分类防护控制项

信息类型		防护环节									
		身份认证	传输安全	存储安全		应用安全					安全审计
				分类存储	备份与恢复	信息发布审核	网页防篡改	授权与访问控制	分域控制	终端安全	
敏感信息		++	—	—	—	++	—	+	+	+	++
公开信息	内部公开信息	+	—	—	+	+	—	—	—	+	+
	外部公开信息	—	#	—	—	—	—	#	#	—	—
注：“#”表示未实施；“—”表示实施；“+”表示在“—”的基础上有所加强；“++”表示在“+”的基础上又有所加强。											

B.3 敏感信息防护示例

B.3.1 身份认证

基于身份认证的防护措施主要包括如下两个方面：

a) 存储和处理内部受控信息的政务办公系统实现基于数字证书、生物特征方式或多种方式相结合的身份认证功能。对进行关键操作的用户和管理员采用相应的认证方式；
b) 存储和处理内部受控信息的政务办公系统采用统一身份认证技术，实现单点登录功能。

B.3.2 传输安全

基于传输安全的防护措施主要包括如下 3 个方面：

a) 当政务信息在互联网上传输时，综合采用商用密码、VPN 技术，实现移动安全接入与网络安全互联，提供保密性、完整性与抗重放攻击等服务；
b) 使用的密码算法符合国家有关规定；
c) 所采用的传输设备能够抵御来自互联网用户的攻击，性能满足用户需求。

B.3.3 存储安全

B.3.3.1 信息分域存储

符合信息分类存储要求，将敏感信息单独存放于内部数据处理域。

B.3.3.2 备份与恢复

基于备份与恢复的防护措施主要包括如下两个方面：

a) 建立数据备份和恢复机制，对重要数据进行及时备份和破坏后的恢复；
b) 建立系统备份和恢复机制，对关键的政务服务系统进行备份和破坏后的恢复。

B.3.4 应用安全

B.3.4.1 统一授权与访问控制

基于统一授权与访问控制的防护措施主要包括如下 7 个方面：

a) 对内部受控信息进行统一的标识与管理；
b) 对内部受控信息的权限，按部门进行层次化管理，降低授权管理难度，提高授权效率；
c) 存储和处理内部受控信息的政务办公系统实现基于功能模块和工作流的访问控制功能。依据安全策略对用户的访问行为进行控制，防止未授权访问；
d) 执行关键操作的政务人员必须是通过数字证书或生物特征认证的用户，防止重要业务的操作权限被攻击者非法获取；
e) 访问内部受控信息时履行审批手续，审批合法后方可访问；
f) 执行审批手续的用户必须是通过数字证书或生物特征认证的用户，执行审批操作时需要进行二次身份确认；
g) 执行审批时限定访问时限。

B.3.4.2 分域控制

基于分域控制的防护措施主要包括如下两个方面：

a) 部署分域控制的网络设备，阻止普通互联网用户接入内部数据处理域访问内部信息；
b) 部署分域控制的网络设备，阻止来自公开数据处理域用户、进程和程序接入内部数据处理域访问内部信息。

B.3.4.3 信息处理终端安全

处理内部受控信息的终端应满足终端增强安全应用模式的防护要求。

B.3.5 安全审计

基于安全审计的防护措施主要包括如下两个方面：

a) 对访问内部受控信息的行为进行日志记录和安全事件分析，日志内容应至少包括时间、用户、被访问对象、访问结果等内容；

b) 对访问内部授权信息的审批操作进行日志记录，日志内容至少包括访问审批人员、审批时间、审批结果、访问者、访问时限等内容。

B.4 内部公开信息防护示例

B.4.1 身份认证

基于身份认证的防护措施主要包括如下两个方面：

a) 存储和处理内部共享信息的政务办公系统实现基于口令、数字证书、生物特征方式或多种方式相结合的身份认证功能。普通人员采用口令认证方式，对进行关键操作的用户和管理员采用数字证书或生物特征认证方式；

b) 存储和处理内部共享信息的政务办公系统采用统一身份认证技术，实现单点登录功能。

B.4.2 传输安全

基于传输安全的防护措施主要包括如下 3 个方面：

a) 当政务信息在互联网上传输时，综合采用商用密码、VPN 技术，实现移动安全接入与网络安全互联，提供保密性、完整性与抗重放攻击等服务；

b) 使用的密码算法符合国家有关规定；

c) 所采用的传输设备能够抵御来自互联网用户的攻击，性能满足用户需求。

B.4.3 存储安全

B.4.3.1 信息分域存储

符合安全信息分域存储要求，将内部共享信息单独存放于内部数据处理域。

B.4.3.2 备份与恢复

基于备份与恢复的防护措施主要包括如下两个方面：

a) 建立数据备份和恢复机制，对重要数据进行及时备份和破坏后的恢复；

b) 建立系统备份和恢复机制，对关键的政务服务系统进行备份和破坏后的恢复。

B.4.4 应用安全

B.4.4.1 统一授权与访问控制

基于统一授权与访问控制的防护措施主要包括如下 4 个方面：

a) 对内部共享信息进行统一的标识与管理；

b) 对内部共享信息的权限，按部门进行层次化管理，降低授权管理难度，提高授权效率；

c) 存储和处理内部共享信息的政务办公系统实现基于功能模块和工作流的访问控制功能。依据安全策略对用户的访问行为进行控制，防止未授权访问；

d) 执行关键操作的政务人员必须是通过数字证书或生物特征认证的用户，防止重要业务的操作权限被攻击者非法获取。

B.4.4.2 分域控制

基于分域控制的防护措施主要包括如下两个方面：

a) 部署分域控制的网络设备，阻止普通互联网用户接入内部数据处理域访问内部信息；

b) 部署分域控制的网络设备，阻止来自公开数据处理域用户、进程和程序接入内部数据处理区访问内部信息。

B.4.4.3 信息处理终端安全

基于信息处理终端安全的防护措施主要包括如下两个方面：

a) 处理内部共享信息的终端应满足终端基本安全应用模式的防护要求；

b) 处理内部共享信息的移动终端应满足便携式终端安全应用模式的防护要求。

B.4.5 安全审计

对执行重要操作的行为应进行日志记录和安全事件分析，日志内容应至少包括时间、用户、被访问对象、访问结果等内容，方便进行事后追踪与责任认定。

B.5 外部公开信息防护示例

B.5.1 身份认证

存储和处理公开信息的政务服务系统实现基于口令方式的身份认证功能，对信息的发布者和管理者进行基于口令的身份认证，对信息的访问者和其余人员不进行身份认证。

B.5.2 存储安全

B.5.2.1 信息分类存储

符合安全信息分类存储要求，将公开信息单独存放于公开数据处理域。

B.5.2.2 备份与恢复

建立系统备份和恢复机制，对关键的政务服务系统进行备份和破坏后的恢复。

B.5.3 应用安全

B.5.3.1 信息发布审核

基于信息发布审核的防护措施主要包括如下 4 个方面：

a) 设置信息发布审核管理员角色，对发布信息的内容进行审查；

b) 信息发布审核管理员角色，应是持数字证书的用户；

c) 面向公众发布的信息要经过管理员审核，只有经过审核的信息才能向公众发布；

d) 依照《中华人民共和国保守国家秘密法》以及其他法律、法规和国家有关规定对拟公开的政府信息进行审查。

B.5.3.2 信息安全交换

由于业务需要，行政审批、投诉等公开信息会进入到内部数据处理域进行办理，此时公开数据处理域和内部数据处理域之间的信息处理应符合信息安全交换要求。

B.5.3.3 网页防篡改

部署网页防篡改系统，对非法篡改行为进行实时检测，及时恢复正确网页，产生报警信息。

B.5.3.4 信息处理终端安全防护

存储和处理公开信息的政务服务系统应安装防病毒软件，防止病毒传播。

B.5.4 安全审计

对政务信息的发布操作应进行日志记录，日志内容至少包括发布审批人员、审批时间、审批结果、信息发布人员、发布信息内容等内容。

中 华 人 民 共 和 国
国家标准化指导性技术文件

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

GB/Z 24294.1—2018

*

中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)

网址：www.spc.org.cn
服务热线：400-168-0010

2018年3月第一版

*

书号：155066·1-59627

GB/Z 24294.1-2018