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 24294.2—2017
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2部分:接入控制与安全交换

Information security technology—Guide of implementation for Internet-based e-government information security—Part 2:Access control and secure exchange

2017-05-31 发布　　2017-12-01 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4个部分：

——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2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《信息安全技术　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：

——给出了接入控制组成结构与实施办法；

——对接入控制功能、网络适应性提出了新的基本要求，详细细化了接入认证、接入控制规则以及接入控制管理要求，更加适合电子政务安全接入控制需求；

——针对安全交换补充了信息安全交换模式分类；

——针对安全交换补充了定制数据安全交换模式技术要求和数据流安全交换模式技术要求。

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所、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、夏春涛、曹利峰、张东巍、任志宇、罗锋盈、上官晓丽、董国华。

本部分所代替标准的历次版本发布情况为：

——GB/Z 24294—2009。

引　言

互联网作为我国电子政务的重要信息基础设施，尽管提高了办公的效率，节约了资源与成本，但是互联网的开放性，接入用户、接入终端、接入手段的多样化，电子政务系统的安全要求与电子政务系统的开放性之间的矛盾等，将使得电子政务系统面临着非法接入、非授权访问、信息无法安全共享等安全问题，应该引起高度重视。为确保政务用户能够合法接入互联网电子政务系统安全区域，防止非法接入与非授权访问，以及域间信息安全交换特制定本部分，推动互联网在我国电子政务中的安全应用。

本部分提出了安全接入与安全交换两个阶段的安全功能要求，对基于互联网电子政务信息安全系统结构设计、网络接入方式、信息安全共享提供指导。本部分首先对分域控制与域间信息安全交换模式进行描述，然后分别从接入控制和信息安全交换技术两个阶段进行描述。在接入控制阶段，首先对接入控制模式进行了描述，明确了接入控制的组成、功能以及接入方式的要求；接着对接入认证、分域控制要求进行了规范，明确了接入认证、接入设备功能等要求，并描述了分域控制实施细则；最后对接入控制规则、接入管理进行了描述，明确了不同情况下接入控制策略以及安全管理要求。在安全交换阶段，首先对互联网电子政务信息安全交换的安全需求进行描述；明确了基于互联网电子政务信息安全交换的模式；然后分别对在定制数据安全交换模式和数据流安全交换模式下实施信息安全交换的关键环节提出相关要求。

本部分主要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，基于互联网开展非涉及国家秘密的电子政务建设，当建设需要时，可根据安全策略与电子政务外网进行安全对接。

信息安全技术
基于互联网电子政务信息安全实施指南
第2部分:接入控制与安全交换

1 范围

GB/Z 24294的本部分明确了互联网电子政务分域控制的两个阶段,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要求;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要求。

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安全接入控制策略设计、工程实施与系统研发,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规划与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。

GM/T 0022—2014 IPsec VPN技术规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

接入鉴别方式 access authentication method

对接入主体进行身份合法性检查所采用的方法与手段,以保证接入主体的合法性。

3.2

接入控制规则 access control rule

针对不同的接入主体,制定相应的安全规则,防止接入主体对内部网络资源的非法访问和越权访问。

3.3

接入主体组 access subject group

将属于同一安全域内的用户、主机、子网、地址段、物理网络接口、服务等按照相同的访问属性归属为同一个组,每个组内成员访问的资源内容是相同的,组由组对象名来标识。

3.4

接入主体 access subject

能够接入到内部网络中的终端用户、设备、区域、网段等。接入到内部网络的访问者均有相应的别名,该别名被称为对象名。