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 24294.4—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4部分:终端安全防护

Information security technology—Guide of implementation for Internet-based e-government information security—Part 4:Defense for terminal security

2017-05-12 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4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：

——新增了基于互联网电子政务终端的脆弱点和面临的主要威胁；

——补充明确了基于互联网电子政务终端的安全防护功能和实施原则；

——补充了划分基于互联网电子政务终端安全防护的主要应用模式；

——补充规范了基于互联网电子政务终端在三种应用模式下的安全防护要求。

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，计算机终端在电子政务系统中承担和参与政务信息的处理、存储和传输等重要工作，面临着恶意代码、网络攻击、信息泄漏和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终端安全防护工作，特制定本部分。

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，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4部分:终端安全防护

1 范围

GB/Z 24294的本部分按照终端安全防护策略,明确了基于互联网电子政务终端的安全防护技术要求。

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 30278—2013 信息安全技术 政务计算机终端核心配置规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

安全政务终端 terminal for secure government affairs

满足政务办公安全防护技术要求,能够开展政务办公与业务应用的计算机终端和手持式终端。

4 缩略语

下列缩略语适用于本文件。

FTP 文件传输协议(File Transfer Protocol)

IIS 互联网信息服务(Internet Information Services)

IP 互联网协议(Internet Protocol)

WWW 万维网(World Wide Web)

5 终端安全功能与实施原则

5.1 安全脆弱点

计算机终端作为基于互联网电子政务系统的基本工作单元,承担和参与政务信息的加工、处理、存储和传输等重要工作,主要安全威胁和脆弱点包括: