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:

a) 互联网恶意攻击——基于互联网电子政务终端极易遭受来自互联网的病毒、木马等恶意代码攻击，将会导致政务终端产生信息泄漏、身份假冒、虚假消息发布和工作效率降低等安全风险。

b) 补丁升级滞后——操作系统、应用软件漏洞补丁不能及时更新，将会给病毒和木马等恶意代码带来可乘之机，进而威胁整个应用系统。

c) 终端非法接入——当非授权终端接入电子政务系统进行政务办公访问网络资源时，会对政务网络、合法终端以及应用系统带来安全隐患。

d) 系统安全配置不合理——操作系统安全配置项如果不能进行合理的选择和部署，不仅消弱系统自身的防护能力，降低防范的实施效率，同时造成维护成本的增加。

5.2 安全功能

基于互联网电子政务终端围绕统一安全策略，需实现核心安全配置、状态实时监测、系统补丁升级、恶意代码查杀和用户操作审计等功能，构建安全政务终端。主要功能包括：

a) 核心安全配置——核心安全配置适用于使用 windows 操作系统的终端，对终端的账户密码策略、账户锁定策略、本地审核策略、本地用户权限指派、事件日志、IE 安全配置和系统服务等项进行配置，加固操作系统。

b) 状态实时监测——管理员可以实时监测到终端运行状态，实现对接入政务网络终端的实时管理和维护，终端状态包括运行进程、启动服务和网络连接等信息。

c) 系统软件升级——计算机终端系统软件和主要应用软件的升级宜及时和安全，通过监测终端的漏洞和补丁等信息，由统一的补丁漏洞管理平台自动下发给终端。

d) 恶意代码查杀——为防范恶意代码，宜采用杀毒引擎阻断未知病毒和网络入侵。恶意代码查杀包括有效清除木马、蠕虫、后门、流氓软件、间谍软件、广告程序、ARP 病毒和网页挂马等威胁。

e) 用户操作审计——对终端用户和管理员用户的行为进行识别、记录、存储和分析，为安全管理人员和决策者提供有效数据，同时具有告警功能，便于事件分析调查、适时调整安全策略。

5.3 实施原则

基于互联网电子政务终端安全防护的实施原则包括：

a) 适度安全——政务终端应根据不同的安全应用模式采用适度的安全防护措施，合理配置和部署，进行有效管理和实施。

b) 操作方便——充分考虑到我国信息安全技术发展和应用现状，基于互联网电子政务终端安全防护措施应易于实施，操作方便。

c) 兼容性——终端安全防护产品与电子政务办公系统应具有兼容性，避免因终端安全防护措施导致政务办公无法实施的现象发生。

6 终端安全应用模式

6.1 终端基本安全应用模式

大多数计算机终端在政务办公时终端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，不涉及或很少涉及政务办公中的内部受控信息。这部分终端宜采用基本安全应用模式。该模式提供政务办公所需的基本安全防护功能，满足 GB/T 30278—2013 的要求，是基于互联网电子政务终端安全防护的基础。

6.2 终端增强安全应用模式

部分计算机终端在政务办公中需要处理或涉及大量敏感信息，这类终端的防护，除了具备基本安全防护外，还需要实施终端增强安全防护，只有安全性评估合格的终端才允许接入政务网络。该应用模式提供了政务办公的增强安全防护。

6.3 移动终端安全应用模式

当政务人员在移动环境中使用便携式终端或手持式终端进行政务办公时，适宜采用移动终端安全应用模式。便携式终端通过构建独立于宿主机的操作系统和办公应用软件，以及隔离于宿主机硬盘的安全存储区来实现终端安全防护；手持式终端通过终端安全模块在数据安全、用户身份鉴别和设备控制等方面来实现终端安全防护。

7 终端基本安全防护要求

7.1 系统服务配置

主要内容包括：

a) 禁用 Alerter 服务。终端用户不需要接受来自计算机系统管理级警报(AdministrativeAlerts)。
b) 禁用 ClipBook 服务。禁止与远程电脑共享剪贴板内容。
c) 禁用 FTP Publishing Service。禁止开启 FTP 服务。
d) 禁用 IIS Admin Service。禁用 IIS 管理。
e) 禁用 Messenger 。禁用信使服务。
f) 禁用 NetMeeting Remote Desktop Sharing 。禁用 netmeeting 远程桌面共享
g) 禁用 Routing and Remote Access 。禁用软件路由器功能
h) 禁用 SSDP Discovery Service 。禁用简易服务发现协议 SSDP 的服务，该服务用于家庭网络中的 UPnP 设备的发现。
i) 禁用 Telnet 。禁用 Telnet 服务。
j) 禁用 World Wide Web Publishing Services。禁用 WWW 服务。

7.2 账户策略配置

7.2.1 账户口令策略

主要内容包括：

a) 口令符合复杂性要求宜启用；
b) 口令长度最小值宜设置为不小于 8 位；
c) 强制口令历史的次数宜设置为不小于 6。

7.2.2 账户锁定策略

主要内容包括：

a) 账户锁定阈值，即用户账户被锁定的登录尝试失败的次数不大于 5；
b) 账户锁定时间，即锁定账户在自动解锁之前保持锁定的分钟数不小于 15。

7.3 日志与审核策略配置

7.3.1 事件日志

主要内容包括：

a） 设置系统日志、安全日志和应用日志的最大字节分别不小于16 384 KB、81 920 KB和16 384 KB；
b） 禁止本地 Guests 组访问系统日志、安全日志和应用日志；
c） 设置系统日志、安全日志和应用日志的保留方法为按需要覆盖事件，且不能定义日志的保留天数。

7.3.2 本地审核

主要内容包括：
a） 审核账户登录事件，即在本地账户登录成功时和失败时生成审核项。
b） 审核特权使用，即在用户权限执行失败时生成审核项。
c） 审核策略更改，即在成功更改用户权限分配策略、审核策略或信任策略时生成审核项。
d） 审核系统事件，即在系统事件执行成功时生成审核项。系统事件包括用户重新启动或关闭计算机时或者在发生影响系统安全或安全日志的事件等。
e） 审核账户管理，即审核计算机上的每个账户管理事件的成功和失败操作。

7.4 浏览器安全配置

对管理模板中 windows 组件中的 Internet Explorer 进行安全配置，主要内容包括：
a） 禁止 Internet Explorer 自动安装组件。
b） 禁止 Internet Explorer 检查是否有新版本。
c） 禁用程序启动时的软件更新通知。如果启用该策略，则在使用软件分发频道更新程序时，用户将不会被通知而程序自动进行更新操作。如果禁用该策略或不对其进行配置，则在更新程序之前用户将收到通知。
d） 禁止用户启用或禁用加载项。
e） 关闭故障检测。
f） 启用 IE 进程的限制 ActiveX 功能，阻止 Internet Explorer 进程的 ActiveX 控件安装提示。

7.5 恶意代码防范

终端宜安装和运行恶意代码防范系统并及时更新病毒库，定期进行恶意代码扫描和清除，防范恶意代码的扩散。

7.6 个人防火墙

终端宜安装并运行个人防火墙系统，依据安全策略，实现对进出计算机的数据包进行安全过滤，同时支持用户策略的统一配置。

7.7 系统漏洞补丁升级

终端在首次安装时不含恶意软件，在使用过程中确保及时安装已发布的系统漏洞补丁。漏洞补丁包含：
a） 操作系统关键补丁。对微软发布的 winXP、Vista 和 win7 等操作系统的漏洞补丁宜及时安装。
b） 主要软件关键补丁。对浏览器和办公软件等主要应用软件的漏洞补丁宜及时安装。

8 终端增强安全防护要求

8.1 安全性检测

8.1.1 检测目标

终端安全性检测的目标是通过检查终端安全防护措施和安全配置，阻止防护措施不符合规范的终

端接入政务办公应用系统，降低基于互联网电子政务系统所受的安全风险。同时为安全管理员提升终端安全防护能力提供整改依据。

8.1.2 检测指标

检测指标包括：终端的操作系统漏洞补丁、防火墙启动状态、杀毒软件病毒库更新日期以及windows终端核心安全配置等信息。检测按照执行时段包括：在终端操作系统启动之后至政务办公之前的初始检测，以及在政务办公过程之中的实时检测。

8.1.3 检测处理

主要内容包括：

a) 安全性检测结果为合格或不合格。合格者允许接入政务办公系统进行通信，否则不允许接入政务办公系统，同时将检测结果及时提交给安全管理员以便整改。

b) 终端宜设置安全系统恢复区域，当终端检测不合格时，可以使系统自动恢复到安全状态。

8.2 程序运行授权

依据业务需要和安全策略，终端办公使用的政务办公应用程序和安全防护软件如office编辑软件、电子邮件软件、个人防火墙、恶意代码防范软件等宜提交给管理系统进行授权，形成终端程序白名单，经过授权的白名单中的终端应用程序才可以运行。

8.3 安全电子邮件

主要内容包括：

a) 传输安全。支持邮件传输的保密性、完整性和可鉴别性等安全服务，防止政务邮件在传输过程中的泄密、伪造和篡改等；

b) 邮件互发。支持同一安全域内安全邮件的群发，支持基于公钥技术的点对点邮件互发；

c) 密钥管理。支持密钥及用户证书的更新、撤销、恢复、同步等功能。

8.4 安全公文包

主要内容包括：

a) 加密存储要求。支持信息的加密存储保护，支持对安全公文包访问的身份认证，以及数据文件、数据目录的机密性、完整性和数字签名保护；支持与微软Windows系列操作系统的无缝集成。

b) 算法要求。支持国产密码SM1、SM3算法，符合国家商用密码管理条例。

c) 密钥管理。支持密钥的更新、撤销、恢复、同步等密钥管理功能。

8.5 安全审计

主要内容包括：

a) 行为审计。支持对终端用户操作行为事件的审计，如用户上网行为和政务信息处理行为等，与基本安全防护要求中日志与审核策略保持一致。

b) 配置审计。支持对终端安全配置信息更改事件的审计，与基本安全防护要求中日志与审核策略保持一致。

c) 评估审计。支持对终端可信评估结果为不合格事件的审计。

d) 审计数据安全。支持审计数据免遭未经授权的删除或修改。支持审计数据的集中管理。

9 移动终端安全防护要求

9.1 便携式终端安全

9.1.1 系统组成

主要内容包括：

a) 以移动存储介质为载体的操作系统和办公应用软件。这是政务办公的软件环境，宜根据业务需要和安全需求定制。软件环境包含了定制的操作系统、办公应用软件、特定加密存储区域以及相关密码算法；移动存储介质通过 USB 接口与宿主机连接。

b) 宿主机。这是政务办公的硬件环境，它是终端安全防护能力未经验证的不安全终端硬件设备。

c) 安全防护管理平台。主要完成移动存储介质注册与管理、操作系统定制、办公软件定制等功能。

9.1.2 系统隔离

主要内容包括：

a) 操作系统隔离。在宿主机硬件支撑下，移动存储介质上定制的嵌入式操作系统启动后，宜独立于宿主机操作系统，不与宿主机上的系统软件与应用软件通信。

b) 存储系统隔离。移动终端安全应用模式中产生和接收的政务信息宜存储在移动存储介质中的特定加密存储区域，存储过程不受宿主机干扰。

9.1.3 系统功能

9.1.3.1 自身安全

便携式终端安全防护中所使用的自定制系统宜具有嵌入式操作系统漏洞补丁更新、恶意代码特征库升级、系统安全核心配置等功能，支持自定制操作系统安全加固。

9.1.3.2 加密存储

主要内容包括：

a) 算法要求。按照国家规定的商密算法进行安全存储区域中数据的加解密。

b) 效率要求。数据存储在 USB 安全存储区，为不影响正常的办公效率，数据的加解密速率宜不低于 7.0 Mbit/s。

c) 电气特性。支持 USB2.0 及其以上。

9.1.3.3 安全审计

主要内容包括：

a) 进程审计。包含终端执行的主要程序和进程事件。

b) 网络审计。包含终端访问的网络地址事件。

c) 外设审计。包含终端通过 USB 接口使用的外部设备事件。

d) 登录审计。支持基于用户的登录事件。

9.1.3.4 办公软件定制

根据终端政务办公需要，宜支持安装或卸载政务办公所需的各类应用软件，及其相关功能配置。

9.2 手持式终端安全

9.2.1 系统安全

手持式终端宜采用国内具有自主知识产权的终端操作系统，提升系统自身安全，宜支持沙箱等功能实现计算环境隔离。

9.2.2 数据安全

主要内容包括：

a） 密码服务。终端宜提供数字证书管理、数据加解密、数字签名和消息完整性检验等密码服务。

b） 算法要求。按照国家密码管理局批准的密码算法提供密码服务。

9.2.3 身份鉴别

用户身份宜采用双因子强认证，并进行弱口令检测及告警。

9.2.4 设备控制

主要内容包括：

a） 接口控制。宜对 WiFi、蓝牙和 USB 调试等接口进行控制。

b） 外设控制。宜对摄像头和麦克风等接口进行控制。

9.2.5 异常处理

终端宜支持设备异常时的应急处理，包括远程锁定、远程擦除设备数据。

9.2.6 安全审计

审计信息包括操作系统登录/退出、软件安装、程序调用、网络资源访问、通信资源使用和外设使用等。

参 考 文 献

[1] GB/T 20269 信息安全技术 信息系统安全管理要求
[2] GB/T 20984 信息安全技术 信息安全风险评估规范
[3] GB/T 22081 信息技术 安全技术 信息安全管理实用规则

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 4 部分：终端安全防护
GB/Z 24294.4—2017
*
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.net.cn
总编室：(010)68533533　发行中心：(010)51780238
读者服务部：(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 1　字数 18 千字
2017 年 5 月第一版　2017 年 5 月第一次印刷
*
书号：155066·1-55838　定价　18.00 元

GB/Z 24294.4-2017