ICS 35.040
L 80

中华人民共和国国家标准

GB/T 35283—2017

信息安全技术
计算机终端核心配置基线结构规范

Information security techniques—Specification for the structure of desktop core configuration baseline

2017-12-29 发布　　2018-07-01 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

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:国家信息中心、中国信息安全测评中心、中国科学院大学、公安部科信局信息中心、中国民航局信息中心、北京北信源软件股份有限公司、华为技术有限公司、杭州盈高科技有限公司。

本标准主要起草人:李新友、刘蓓、许涛、蔡军霞、王啸天、程浩、付红燕、李守鹏、张涛、张玉清、袁义芳、刘蕴、孙立华、胡东宏、林皓、王盾、贺韬。

引　言

对计算机终端操作系统、办公软件、浏览器等基础软件进行核心配置管理，可有效封堵系统安全漏洞，增强终端的安全可控性，保护数据安全和用户隐私，提高我国政府和企事业单位的计算机终端整体安全水平。

政务终端核心配置系列标准是依据我国信息安全等(分)级保护要求，基于我国政务终端安全保障实际需求，并借鉴国外相关研究成果提出的。该系列标准中 GB/T 30278—2013《信息安全技术　政务计算机终端核心配置规范》已经颁布并实施，其规定了政务计算机终端核心配置的基本概念和要求，核心配置的自动化实现方法，规范了核心配置实施流程，并为本标准提供依据。本标准在研究 Windows 安全配置方法的基础上，借鉴其他操作系统安全配置方法，规定了计算机核心配置基线的结构及各层元素的标记规则，并给出了基线应用方法实例。核心配置基线根据各单位信息系统安全保护要求制定的计算机终端核心配置策略集，可用于针对大规模计算机终端进行自动化核心配置部署和合规性管理。一方面，技术人员可以参照本标准开发核心配置基线生成及解析工具，用于核心配置基线的自动化部署及监测管理。另一方面，技术人员可以参照本标准规定的基线结构编写新的安全配置基线，从而不断扩展计算机终端安全配置的应用范围，提高自动化应用水平。

信息安全技术
计算机终端核心配置基线结构规范

1 范围

本标准规定了计算机终端核心配置基线的基本要素，规范了基于 XML 的核心配置基线标记规则，并给出了核心配置基线应用方法实例。

本标准适用于计算机终端的核心配置自动化工作，包括计算机终端核心配置自动化工具的设计、开发和应用。

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 19667.1—2005 基于 XML 的电子公文格式规范 第 1 部分：总则

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

GB/T 30278—2013 和 GB/T 19667.1—2005 界定的以及下列术语和定义适用于本文件。

3.1

核心配置项(配置项) core configuration item

计算机操作系统、办公软件、浏览器、BIOS 系统和防恶意代码软件等基础软件中影响计算机安全的关键参数可选项。

注：核心配置项类型包括开关项、枚举项、区间项和复合项，可以根据安全要求对其进行赋值。

[GB/T 30278—2013，定义 3.2]

3.2

核心配置 core configuration

对核心配置项进行参数设置的过程。

注：通过核心配置限制或禁止存在安全隐患或漏洞的功能，启用或加强安全保护功能，来增强计算机抵抗安全风险的能力。

[GB/T 30278—2013，定义 3.3]

3.3

核心配置基线 core configuration baseline

能够满足计算机安全基本要求的一组或多组核心配置项基值构成的集合。

3.4

核心配置基线包 core configuration baseline package

为实现核心配置基线自动化部署而制定的一种具有特定语法格式的核心配置数据文件。

[GB/T 30278—2013，定义 3.7]