



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 发布
中国国家标准化管理委员会

目 次

前言	I
引言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	2
5 核心配置基线基本要素	2
6 基于 XML 的核心配置基线标记规则	3
6.1 核心配置基线结构	3
6.2 第一层元素标记	4
6.3 第二层元素标记	4
6.4 第三层元素标记	5
6.5 第四层元素标记	9
6.6 第五层元素标记	11
6.7 第六层元素标记	12
6.8 第七层元素标记	15
附录 A (资料性附录) 核心配置基线标记完整示例	17
附录 B (资料性附录) 核心配置基线标记应用示例	21
B.1 “口令长度最小值为 8 位字符长度”核心配置基线 XML 示例	21
B.2 “口令长度最小值为 8 位字符长度”核心配置基线 XML 示例简要说明	23
附录 C (资料性附录) 核心配置基线应用示例	24
C.1 核心配置编辑	24
C.2 核心配置验证	27
C.3 核心配置部署	28
C.4 核心配置监测	30
参考文献	31



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、杭州盈高科技技术有限公司。

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]

3.5

元素 element

某个数据集内的一个具体数据项。

[GB/T 19667.1—2005,定义 3.7]

3.6

属性 attribute

给一个具体元素实例添加信息或修改其信息的一个名称。

[GB/T 19667.1—2005,定义 3.8]

4 缩略语

下列缩略语适用于本文件。

CGDCC:政务计算机终端核心配置(Chinese Government Desktop Core Configuration)

XML:可扩展标记语言(Extensible Markup Language)

WMI:Windows 管理规范(Windows Management Instrumentation)

GUID:全局唯一标识符(Globally Unique Identifier)

5 核心配置基线基本要素

核心配置基线主要包括如下四个基本要素：

- a) 产品信息：主要描述基线适用的操作系统或软件环境，如操作系统版本、软件名称等。一般不同的产品对应不同的基线；
- b) 配置项信息：是核心配置基线的基本构成元素，主要描述配置项的内容、取值和检查规则等属性；
- c) 配置组信息：主要将基线中所有配置项按照安全功能进行分组。一条核心配置基线通常包含多个配置组，一个配置组包含多个配置项；
- d) 版本信息：主要标识一条核心配置基线的结构或内容经过修改变化的过程，如基线格式版本、基线版本、配置组版本、配置项版本和产品版本等。

产品信息、配置组信息、配置项信息和版本信息四要素的关系如图 1 所示。

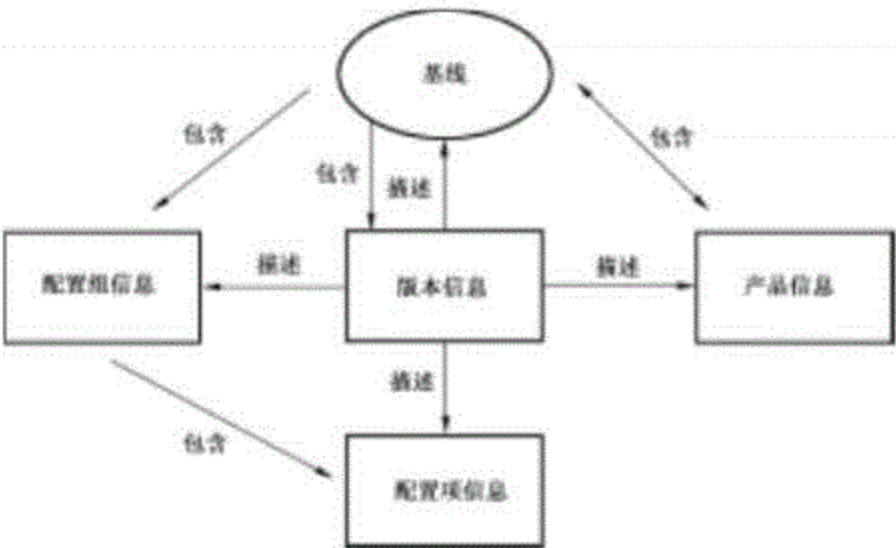


图 1 基线四要素关系图

6 基于 XML 的核心配置基线标记规则

6.1 核心配置基线结构

核心配置基线是一种嵌套式结构的数据文件,主要采用 XML 格式对核心配置项的属性进行规范性标记,其标记完整示例参见附录 A。根据 GB/T 19667.1—2005 第 8 章的规定,完整的核心配置基线可表示为七层元素嵌套结构,每层元素中由上层元素衍生出来的元素,称为上层元素的子元素,如图 2 所示。其中,适用产品标记主要描述产品要素,配置组别主要描述配置组要素,配置项内容标记主要用于描述配置项要素,格式版本标记、版本控制标记、基线版本编号标记、配置组版本编号标记、配置项版本编号标记和操作系统版本标记分别描述基线、配置组、配置项和产品的版本要素。

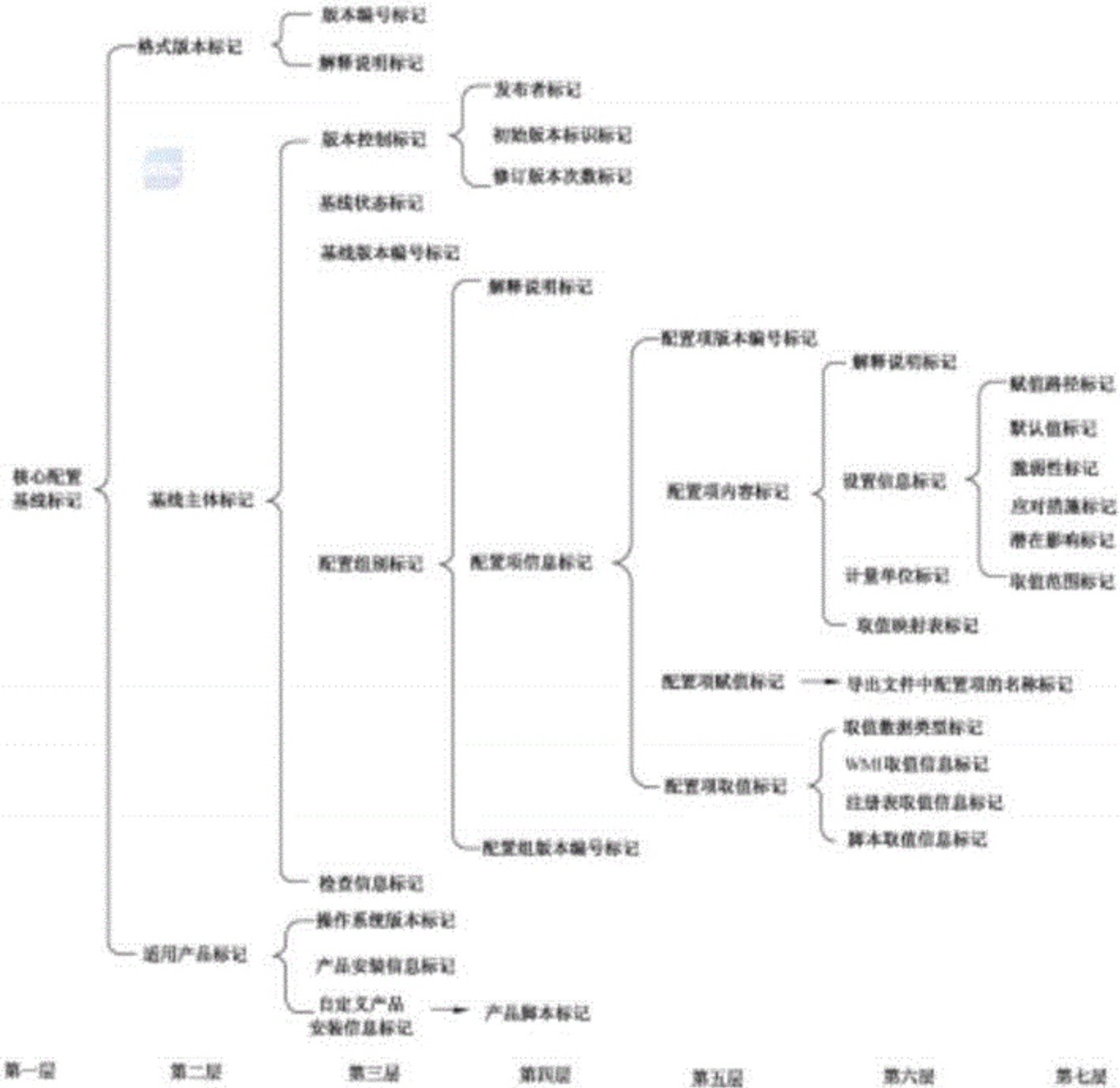


图 2 核心配置基线结构

第一层元素为核心配置基线包标记,其标记规则见 6.2。

第二层元素包括格式版本标记、基线主体标记和适用产品标记，其标记规则见 6.3。

第三层包含十个元素。其中，版本编号标记和解释说明标记为格式版本标记的子元素，标记规则见 6.4.1；版本控制标记、基线状态标记、基线版本编号标记、配置组别标记和检查信息标记为基线主体标记的子元素，标记规则见 6.4.2；操作系统版本标记、产品安装信息标记和自定义产品安装信息标记为适用产品标记的子元素，标记规则见 6.4.3。

第四层包含七个元素。其中，发布者标记、初始版本标识标记和修订版本次数标记为版本控制标记的子元素，标记规则见 6.5.1；解释说明标记、配置项信息标记和配置组版本编号标记为配置组别标记的子元素，标记规则见 6.5.2；产品脚本标记为自定义产品安装信息标记的子元素，标记规则见 6.5.3。

第五层包含四个元素。其中，配置项版本编号标记、配置项内容标记、配置项赋值标记和配置项取值标记为配置项信息标记的子元素，标记规则见 6.6。

第六层包含九个元素。其中，解释说明标记、设置信息标记、计量单位标记、和取值映射表标记为配置项内容标记的子元素，标记规则见 6.7.1；取值数据类型标记、WMI 取值信息标记、注册表取值信息标记和版本取值信息标记为配置项取值标记的子元素，标记规则见 6.7.2；导出文件中配置项的名称标记为配置项赋值标记的子元素，标记规则见 6.7.3。

第七层包含六个元素，其中赋值路径标记、默认值标记、脆弱性标记、应对措施标记、潜在影响标记和取值范围标记为设置信息标记的子元素，标记规则见 6.8。

计算机核心配置基线的结构及各层元素的标记规则是制定核心配置基线的基础，用户根据各单位信息系统安全保护要求制定基线，并对计算机终端进行自动化核心配置部署和合规性管理。核心配置基线标记应用示例参见附录 B，核心配置基线应用示例参见附录 C。

6.2 第一层元素标记

第一层元素为核心配置基线标记，具体格式定义如表 1 所示。

表 1 第一层元素标记

序号	名称	标记	类型	解释说明
1	核心配置基线标记	CGDCC-Package	元素	用于表示核心配置基线
格式定义源代码： <xs:element name="CGDCC-Package" type="PackageType"/>				

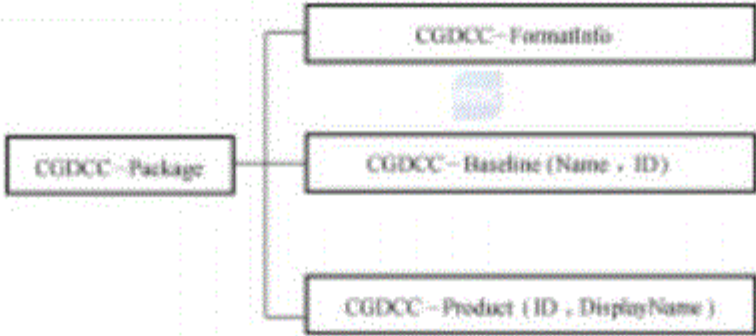
6.3 第二层元素标记

第二层元素包括格式版本标记、基线主体标记和适用产品标记。其中，基线主体标记的属性包括基线名称标记和基线标识标记。适用产品标记的属性包括产品标识标记和产品名称标记。具体格式定义如表 2 所示。

表 2 第二层元素标记

序号	名称	标记	类型	解释说明
1	格式版本标记	CGDCC-FormatInfo	元素	描述核心配置基线格式版本的信息
2	基线主体标记	CGDCC-Baseline	元素	描述核心配置基线的分发及部署信息，可以描述多条基线
	基线名称标记	Name	属性	描述核心配置基线名称
	基线标识标记	ID	属性	描述核心配置基线唯一标识。此标识按照唯一标识(GUID)生成规则自动生成

表 2 (续)

序号	名称	标记	类型	解释说明
3	适用产品标记	CGDCC-Product	元素	描述核心配置基线适用配置软件产品的范围,可以描述多个产品信息
	产品标识标记	ID	属性	描述软件产品的唯一标识(GUID)
	产品名称标记	DisplayName	属性	描述软件产品的名称
XML 结构模型:				
				
格式定义源代码:				
<pre><xs:complexType name="CGDCC-Package"> <xs:sequence> <xs:element name="CGDCC-FormatInfo"/> <xs:element ref="CGDCC-Baseline" minOccurs="0" maxOccurs="unbounded"/> <xs:attribute name="ID" type="GUIDType" use="required"/> <xs:attribute name="Name" type="xs:string" use="required"/> <xs:element ref="CGDCC-Product" maxOccurs="unbounded"/> <xs:attribute name="ID" type="cgdcc-core:GUIDType"/> <xs:attribute name="DisplayName" type="xs:string" use="required"/> </xs:sequence> </xs:complexType></pre>				

6.4 第三层元素标记

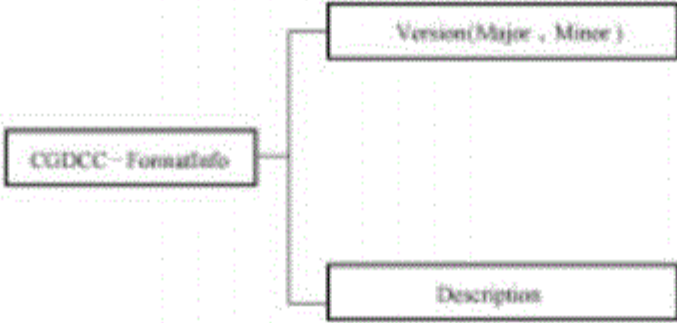
6.4.1 格式版本标记子元素

格式版本标记的子元素包括版本编号标记和解释说明标记。具体格式定义如表 3 所示。

表 3 格式版本标记的子元素

序号	名称	标记	类型	解释说明
1	版本编号标记	Version	元素	核心配置基线格式版本的唯一标识
	主版本号标记	Major	属性	核心配置基线格式主版本号的唯一标识
	子版本号标记	Minor	属性	核心配置基线格式子版本号的唯一标识
2	解释说明标记	Description	元素	对版本规则进行简要说明

表 3 (续)

序号	名称	标记	类型	解释说明
XML 结构模型:				
				
格式定义源代码:				
<pre><xs:element name="CGDCC-FormatInfo"> <xs:complexType> <xs:sequence> <xs:element name="Version"> <xs:attribute name="Major" type="xs:unsignedInt"/> <xs:attribute name="Minor" type="xs:unsignedInt"/> <xs:element name="Description" type="xs:string" minOccurs="0"/> </xs:sequence> </xs:complexType> </xs:element></pre>				

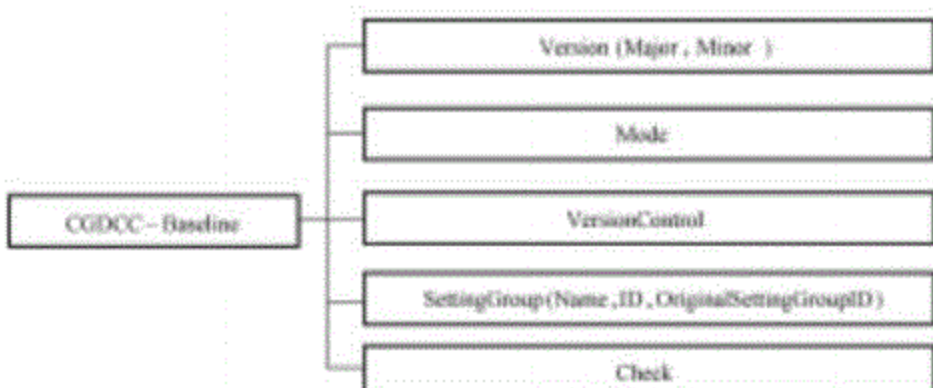
6.4.2 基线主体标记子元素

基线主体标记的子元素包括基线版本编号标记、基线状态标记、版本控制标记、配置组别标记和检查信息标记。具体格式定义如表 4 所示。

表 4 基线主体标记的子元素

序号	名称	标记	类型	解释说明
1	基线版本编号标记	Version	元素	核心配置基线版本的唯一标识
	基线主体主版本号标记	Major	属性	核心配置基线主版本号的唯一标识
	基线主体子版本号标记	Minor	属性	核心配置基线子版本号的唯一标识
2	基线状态标记	Mode	元素	包括可编辑状态和已发布状态两种
3	版本控制标记	VersionControl	元素	描述核心配置基线版本相关信息
4	配置组别标记	SettingGroup	元素	描述核心配置基线所包含的每个策略组的基本信息,可包括多个策略组
	配置组名称标记	Name	属性	描述配置组的名称
	配置组标识标记	ID	属性	描述配置组的唯一标识(GUID)
	初始配置组标识标记	OriginalSettingGroupID	属性	描述初始配置组的唯一标识(GUID)
5	检查信息标记	Check	元素	描述策略组所包含的核心配置项的检查信息,每个配置项都有一条相应的检查信息

表 4 (续)

序号	名称	标记	类型	解释说明
XML 结构模型:				
				
格式定义源代码:				
				<pre><xs:complexType name="CGDCC-BaselineType"> <xs:complexContent> <xs:sequence> <xs:element name="Version" > <xs:attribute name="Major" type="xs:unsignedInt"/> <xs:attribute name="Minor" type="xs:unsignedInt"/> <xs:element name="Mode" type="BaselineModeType"/> <xs:simpleType name="BaselineModeTypes"> <xs:restriction base="xs:string"> <xs:enumeration value="Edit"/> <xs:enumeration value="Published"/> </xs:restriction> </xs:simpleType> <xs:element name="VersionControl" type="BaselineVersionControlType"/> </xs:sequence> </xs:complexType></pre>

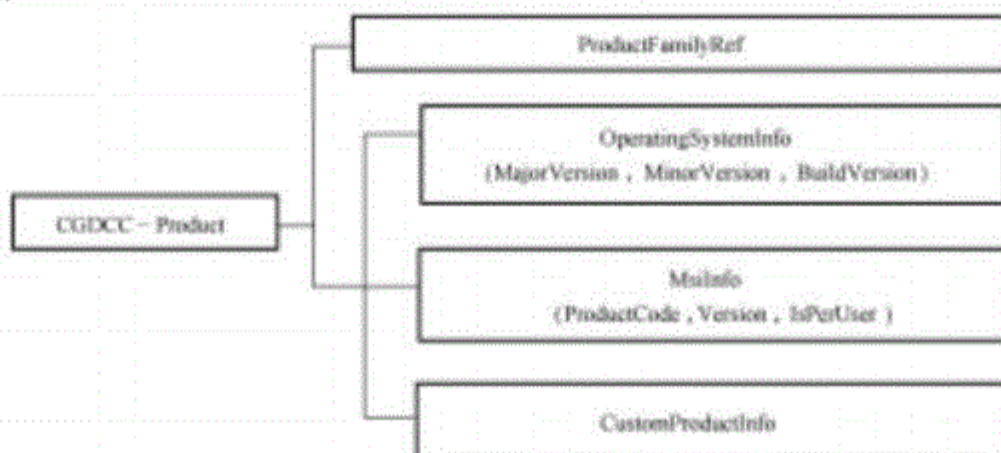
6.4.3 适用产品标记子元素

适用产品标记的子元素标记包括操作系统版本标记、产品安装信息标记、自定义产品安装信息标记和产品家族标记。具体格式定义如表 5 所示。

表 5 适用产品标记的子元素

序号	名称	标记	类型	解释说明
1	操作系统版本标记	OperatingSystemInfo	元素	描述操作系统的版本号
	主版本标记	MajorVersion	属性	描述操作系统有本质改变的编号
	次版本标记	MinorVersion	属性	描述操作系统有较小改变的编号
	编译版本标记	BuildVersion	属性	描述操作系统补丁升级的编号
2	产品安装信息标记	MsiInfo	元素	描述软件产品的安装信息
	产品编号标记	ProductCode	属性	描述产品的标识
	版本标记	Version	属性	描述产品的版本信息
	单用户登录标记	IsPerUser	属性	描述是否支持单用户登录还是多用户登录
3	自定义产品安装信息标记	CustomProductInfo	元素	描述自定义软件产品的安装信息
4	产品家族标记	ProductFamilyRef	元素	描述软件产品所属的产品系列的总称,如 Windows。用 GUID 标识表示

XML 结构模型:



格式定义源代码:

```

<xs:complexType name="ProductType">
  <xs:sequence>
    <xs:choice>
      <xs:element name="OperatingSystemInfo" type="OperatingSystemInfoType"/>
      <xs:attribute name="MajorVersion" type="xs:unsignedInt" use="required"/>
      <xs:attribute name="MinorVersion" type="xs:unsignedInt" use="required"/>
      <xs:attribute name="BuildVersion" type="xs:unsignedInt" use="required"/>
      <xs:element name="MsiInfo" type="MsiInfoType"/>
      <xs:attribute name="ProductCode" type="xs:string" use="required"/>
      <xs:attribute name="Version" type="xs:string" use="optional"/>
      <xs:attribute name="IsPerUser" type="xs:boolean" use="required"/>
      <xs:element name="CustomProductInfo" type="CustomProductInfoType"/>
    
```

表 5 (续)

<pre></xs:choice> <xs:element name="ProductFamilyRef" type="ProductFamilyRefType"> </xs:element></xs:sequence> <xs:documentation> This is product display name, for example, —Windows XP —Windows Vista —Windows Server 2003 —Windows Server 2008 —2007 Office </xs:documentation> <xs:attribute name="ID" type="cgdcc-core:GUIDType"> <xs:attribute name="DisplayName" type="xs:string" use="required"/> </xs:attribute> </xs:complexType></pre>

6.5 第四层元素标记

6.5.1 版本控制标记子元素

版本控制标记的子元素标记包括发布者标记、初始版本标识标记和修订版本次数标记。具体格式定义如表 6 所示。

表 6 版本控制标记的子元素

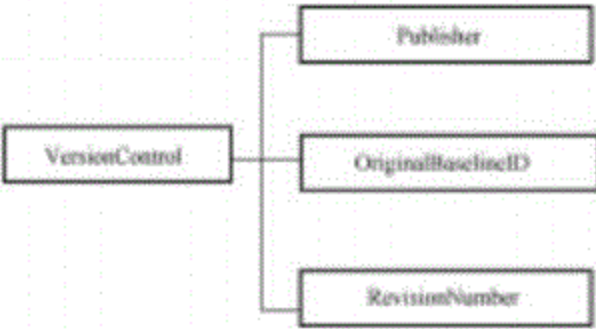
序号	名称	标记	类型	解释说明
1	发布者标记	Publisher	元素	描述发布人信息
2	初始版本标识标记	OriginalBaselineID	元素	描述核心配置基线所第一次生成的标识
3	修订版本次数标记	RevisionNumber	元素	描述从基线第一次生成到目前修订的次数
XML 结构模型:				
				
格式定义源代码:				
<pre><xs:complexType name="BaselineVersionControlType"> <xs:sequence> <xs:element name="Publisher" type="PublisherType"> </xs:element></pre>				

表 6 (续)

<code><xs:element name="OriginalBaselineID" type="cgdcc-core:GUIDType"></code>
<code></xs:element></code>
<code><xs:element name="RevisionNumber" type="xs:unsignedInt"></code>
<code></xs:element></code>
<code><xs:element name="OriginalRevisionNumber" type="xs:unsignedInt"></code>
<code></xs:element></code>
<code></xs:sequence></code>
<code></xs:complexType></code>

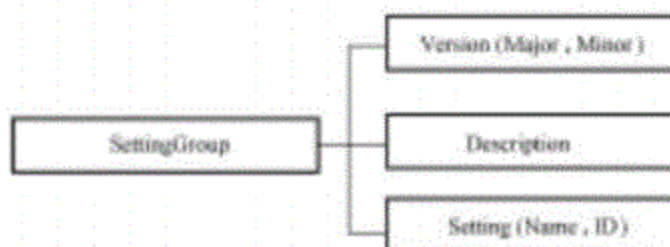
6.5.2 配置组别标记子元素

配置组别标记的子元素标记包括解释说明标记、配置组版本编号标记和配置项信息标记。具体格式定义如表 7 所示。

表 7 配置组别标记的子元素

序号	名称	标记	类型	解释说明
1	解释说明标记	Description	元素	描述配置组的功能介绍
2	配置组版本标记	Version	元素	描述配置组的版本序号
	配置组主版本号标记	Major	属性	描述配置组主版本号的唯一标识
	配置组子版本号标记	Minor	属性	描述配置组子版本号的唯一标识
3	配置项信息标记	Setting	元素	描述配置项的基本信息,可以包含多个配置项
	配置项名称标记	Name	属性	描述配置项的名称
	配置项标识标记	ID	属性	描述配置项的唯一标识(GUID)

XML 结构模型:



格式定义源代码:

```

<xs:complexType name="SettingGroupType">
  <xs:complexContent>
    <xs:extension base="cgdcc-core:NamedObjectBaseType">
      <xs:sequence>
        <xs:element name="Description" type="xs:string" minOccurs="0">
        <xs:element ref="Version">
          <xs:attribute name="Major" type="xs:unsignedInt"/>
          <xs:attribute name="Minor" type="xs:unsignedInt"/>
        <xs:element name="Setting" type="SettingType"/>
      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>
  
```



表 7 (续)

<pre><xs:attribute name="ID" type="GUIDType" use="required"/> <xs:attribute name="Name" type="xs:string" use="required"/> </xs:sequence> </xs:complexContent> </xs:complexType></pre>

6.5.3 自定义产品安装信息标记子元素

自定义产品安装信息标记的子元素为产品脚本标记,具体格式定义如表 8 所示。

表 8 自定义产品安装信息标记的子元素

序号	名称	标记	类型	解释说明
1	产品脚本标记	Script	元素	描述自定义产品安装情况的脚本信息
XML 格式模型:				
				
Schema 定义源代码:				
<pre><xs:complexType name="CustomProductInfoType"> <xs:sequence> <xs:element name="Script" type="cgdce-core:NonEmptyStringType"/> </xs:sequence> </xs:complexType></pre>				

6.6 第五层元素标记

第五层元素为配置项信息标记的子元素,包括版本编号标记、配置项内容标记、配置项取值标记和配置项赋值标记。具体格式定义如表 9 所示。

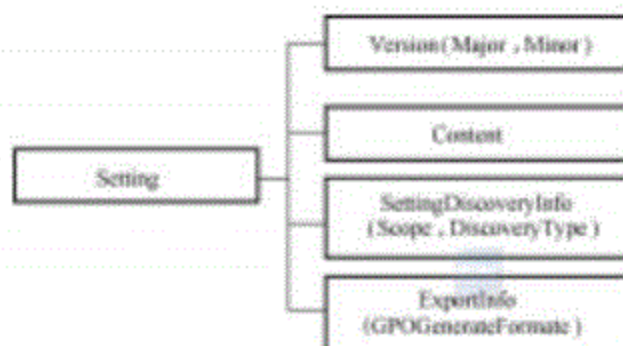
表 9 第五层元素标记

序号	名称	标记	类型	解释说明
1	配置项版本编号标记	Version	元素	核心配置项版本的唯一标识
	配置项主版本号标记	Major	属性	描述配置项主版本号的唯一标识
	配置项子版本号标记	Minor	属性	描述配置项子版本号的唯一标识
2	配置项内容标记	Content	元素	描述配置项内容,包括:赋值路径、脆弱性、应对措施、潜在影响等
3	配置项取值标记	Setting DiscoveryInfo	元素	描述配置项取值类型,包括:作用范围、取值方式、取值数据类型等
	作用范围标记	Scope	属性	指配置项作用范围:本机(Machine)或当前账户(User)
	取值方式标记	DiscoveryType	属性	描述配置项的取值方式,包括 WMI、注册表等

表 9 (续)

序号	名称	标记	类型	解释说明
4	配置项赋值标记	ExportInfo	元素	描述配置项赋值的过程,包括组策略导出文件类型、导出文件中配置项的名称等
	组策略导出文件类型标记	GPOGenerateFormat	属性	描述组策略导出文件的类型,包括 INF、CSV、POL、SCRIPT 四种类型

XML 结构模型:



格式定义源代码:

```

<xs:complexType name="SettingType">
  <xs:complexContent>
    <xs:extension base="cgdccc-core:NamedObjectBaseType">
      <xs:sequence>
        <xs:element ref="Version" />
        <xs:element name="Content" />
        <xs:sequence>
          <xs:element name="SettingDiscoveryInfo" type="SettingDiscoveryInfoType">
            <xs:attribute name="DiscoveryType" type="SettingDiscoveryTypeType" use="required"/>
            <xs:attribute name="Scope" type="SettingScopeType" use="required"/>
          <xs:element name="ExportInfo">
            <xs:attribute name="GPOGenerateFormat" type="GPOGenerateFormatType"
use="required"/>
          </xs:element>
        </xs:sequence>
      </xs:element>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>

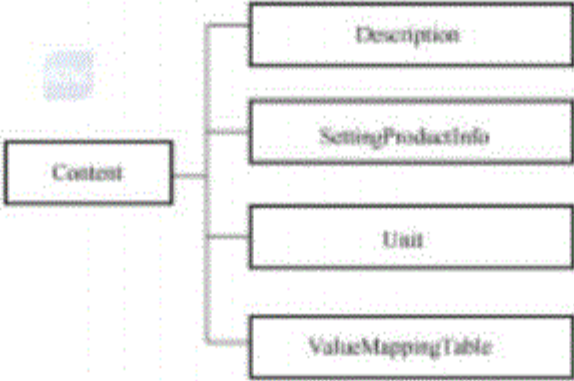
```

6.7 第六层元素标记

6.7.1 配置项内容标记子元素

配置项内容标记的子元素包括解释说明标记、设置信息标记、计量单位标记和取值映射表标记。具体格式定义如表 10 所示。

表 10 配置项内容标记的子元素

序号	名称	标记	类型	解释说明
1	解释说明标记	Description	元素	描述配置项功能及相关参数
2	设置信息标记	SettingProductInfo	元素	描述配置项进行配置时的相关属性
3	计量单位标记	Unit	元素	配置项参数的计量单位
4	取值映射表标记	ValueMappingTable	元素	如果配置项的参数是几个可枚举值,比如是代表颜色的红(0xFF0000)、绿(0x00FF00)和蓝(0x0000FF),括号内为真正取值,此表描述取值与代表此值的显示名称的映射关系,可帮助用户在界面上对取值进行指定
<div>XML 结构模型:</div> <div></div>				
<div>格式定义源代码:</div> <pre><xs:element name="Content"> <xs:complexType> <xs:sequence> <xs:element name="ProductInfo" type="SettingProductInfoType"/> </xs:element> <xs:element name="Unit" type="xs:string"/> </xs:element> <xs:element name="ValueMappingTable"/> </xs:element> <xs:complexContent> <xs:element name="Description" type="xs:string"/> <xs:complexType name="SettingProductInfoType"/> </xs:complexType> </xs:complexType> </xs:element></pre>				

6.7.2 配置项取值标记子元素

配置取值标记的子元素包括取值数据类型标记、WMI 取值信息标记、注册表取值信息标记和脚本取值信息标记。具体格式定义如表 11 所示。

表 11 配置项取值标记的子元素

序号	名称	标记	类型	解释说明
1	取值数据类型标记	DataType	元素	描述配置项取值的数据类型,比如:整型、字符串
2	WMI 取值信息标记	WMIDiscoveryInfo	元素	描述值在 WMI 中的位置
3	注册表取值信息标记	RegistryDiscoveryInfo	元素	描述值在注册表中的位置
4	脚本取值信息标记	ScriptDiscoveryInfo	元素	描述用来取值的脚本

XML 结构模型:

Schema 定义源代码:

```
<xs:complexType name="SettingDiscoveryInfoType">
  <xs:sequence>
    <xs:choice>
      <xs:element name="RegistryDiscoveryInfo" type="cgdcc-core:RegistryDiscoveryType" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element name="WMIDiscoveryInfo" type="cgdcc-core:WMIDiscoveryType"/>
      <xs:element name="ScriptDiscoveryInfo" type="cgdcc-core:ScriptDiscoveryType"/>
    </xs:choice>
    <xs:element name="DataType" type="SettingDataTypes"/>
  </xs:sequence>
</xs:complexType>
```


6.7.3 配置项赋值标记子元素

配置项赋值标记的子元素为导出文件中配置项的名称标记,其属性为导出文件中的段名称标记。在组策略工具中,通过加载组策略导出文件(GPO Backup)进行赋值。其格式定义如表 12 所示。

表 12 配置项赋值标记的子元素

序号	名称	标记	类型	解释说明
1	导出文件中配置项的名称	Inf	元素	组策略导出文件中描述配置项的名称
2	导出文件中的段名称	SectionName	属性	组策略导出文件中描述配置项所在的段的名称

表 12 (续)

XML 格式模型:	
格式定义源代码: <pre><xs:element name="ExportInfo"> <xs:complexType> <xs:sequence> <xs:element name="Inf" minOccurs="0"> <xs:complexType> <xs:attribute name="SectionName" type="xs:string"/> </xs:complexType> </xs:sequence> </xs:complexType> </xs:element></pre>	

6.8 第七层元素标记

第七层元素包括赋值路径标记、默认值标记、脆弱性标记、应对措施标记、潜在影响标记和取值范围标记,为设置信息标记的子元素。具体格式定义如表 13 所示。

表 13 第七层元素标记

序号	名称	标记	类型	解释说明
1	赋值路径标记	UIPath	元素	描述配置项的赋值具体路径
2	默认值标记	DefaultValue	元素	描述在未配置时系统自动设置的值
3	脆弱性标记	Vulnerability	元素	描述该配置项功能所解决的安全风险
4	应对措施标记	CounterMeasure	元素	描述在对不同情况下,如何对配置项参数正确设置
5	潜在影响标记	PotentialImpact	元素	说明启用配置项后可能会造成不确定的影响
6	取值范围标记	ValueRange	元素	允许配置项赋值的范围

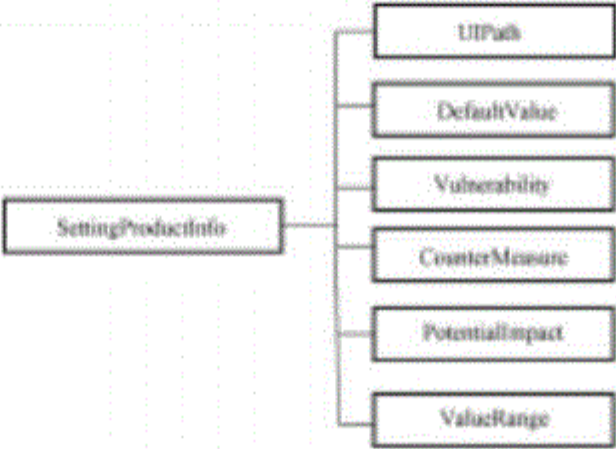
XML 结构模型:	
Schema 定义源代码: <pre><xs:complexType name="SettingProductInfoType"></pre>	

表 13 (续)

```
<xs:sequence>
  <xs:element name="UIPath" type="xs:string" minOccurs="0"/>
  <xs:element name="DefaultValue" type="xs:string"/>
  <xs:element name="Vulnerability" type="xs:string"/>
  <xs:element name="Countermeasure" type="xs:string"/>
  <xs:element name="PotentialImpact" type="xs:string"/>
  <xs:element name="ValueRange" type="SettingNumberValueRangeType" minOccurs="0"/>
</xs:sequence>
</xs:complexType>
```


附 录 A
(资料性附录)
核心配置基线标记完整示例

```

<? xml version = "1.0" encoding = "utf-8"?>
<xs:schema xmlns = "http://schemas.sic.com/CGDCC/SecurityCompliance"
  xmlns:xs = "http://www.w3.org/2001/XMLSchema"
  xmlns:cgdcc-core = "http://schemas.sic.com/CGDCC/SecurityCompliance/core" >
  <xs:complexType name = "CGDCC-PackageType">
    <xs:sequence>
      <xs:element name = "CGDCC-FormatInfo">
        <xs:element name = "CGDCC-FormatInfoType">
          <xs:complexType>
            <xs:sequence>
              <xs:element name = "Version" type = "cgdcc-core:VersionType">
                <xs:complexType name = "VersionType">
                  <xs:attribute name = "Major" type = "xs:unsignedInt"/>
                  <xs:attribute name = "Minor" type = "xs:unsignedInt"/>
                </xs:complexType>
              <xs:element name = "Description" type = "xs:string" minOccurs = "0">
            </xs:element>
          </xs:sequence>
        </xs:complexType>
      <xs:element ref = "CGDCC-Baseline" minOccurs = "0" maxOccurs = "unbounded"/>
      <xs:complexType name = "CGDCC-BaselineType">
        <xs:complexContent>
          <xs:attribute name = "ID" type = "GUIDType" use = "required"/>
          <xs:attribute name = "Name" type = "xs:string" use = "required"/>
        <xs:sequence>
          <xs:element name = "Mode" type = "BaselineModeType"/>
        </xs:sequence>
      </xs:complexType>
    </xs:sequence>
  </xs:complexType>
  <xs:simpleType name = "BaselineModeTypes">
    <xs:restriction base = "xs:string">
      <xs:enumeration value = "Edit"/>
      <xs:enumeration value = "Published"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:element name = "CGDCCVersionControl"
    type = "BaselineVersionControlType"/>
  </xs:element>
  <xs:complexType name = "BaselineVersionControlType">
    <xs:sequence>
      <xs:element name = "Publisher" type = "PublisherType">

```

```

</xs:element>
<xs:element name = "OriginalBaselineID" type = "cgdcc-core:GUIDType">
</xs:element>
<xs:element name = "RevisionNumber" type = "xs:unsignedInt">
</xs:element>
<xs:element name = "OriginalRevisionNumber" type = "xs:unsignedInt">
</xs:element>
</xs:sequence>
</xs:complexType>
  <xs:element ref = "SettingGroup" maxOccurs = "unbounded">
  </xs:element>
<xs:complexType name = "SettingGroupType">
<xs:complexContent>
<xs:extension base = "cgdcc-core:NamedObjectBaseType">
  <xs:sequence>
    <xs:attribute name = "ID" type = "GUIDType" use = "required"/>
    <xs:attribute name = "Name" type = "xs:string" use = "required"/>
  </xs:sequence>
  <xs:attribute name = "OriginalSettingGroupID" type = "cgdcc-core:GUIDType"
use = "required">
  <xs:element name = "Description" type = "xs:string" minOccurs = "0">
  </xs:element>
<xs:complexType name = "SettingType">
<xs:complexContent>
<xs:extension base = "cgdcc-core:NamedObjectBaseType">
<xs:sequence>
  <xs:attribute name = "ID" type = "GUIDType" use = "required"/>
  <xs:attribute name = "Name" type = "xs:string" use = "required"/>
  <xs:element ref = "Version" >
  <xs:element name = "Content">
  <xs:element name = "Content">
<xs:complexType>
<xs:sequence>
  <xs:element name = "ProductInfo" type = "SettingProductInfoType">
  </xs:element>
  <xs:element name = "Unit" type = "xs:string">
  </xs:element>
  <xs:element name = "ValueMappingTable">
  </xs:element>
<xs:complexContent>
  <xs:element name = "Description" type = "xs:string"/>
  </xs:element>
  <xs:complexType name = "SettingProductInfoType">

```

```

<xs:element name = "DiscoveryInfo">
  <xs:complexType>
    <xs:sequence>
      <xs:element name = "SettingDiscoveryInfo" type = "SettingDiscoveryInfoType">
      </xs:element>
      <xs:element name = "DataType" type = "SettingDataTypes">
      </xs:element>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name = "ExportInfo">
  <xs:complexType>
    <xs:sequence>
      <xs:element name = "Inf" minOccurs = "0">
      <xs:complexType>
        <xs:attribute name = "SectionName" type = "xs:string">
        </xs:sequence>
        <xs:attribute name = "GPOGenerateFormat" type = "GPOGenerateFormatType"
use = "required"/>
      </xs:complexType>
    </xs:sequence>
  </xs:complexType>
  </xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:element ref = "CGDCC-Product" maxOccurs = "unbounded"/>
<xs:complexType name = "ProductType">
  <xs:sequence>
    <xs:choice>
      <xs:element name = "OperatingSystemInfo"
type = "OperatingSystemInfoType"/>
      <xs:complexType name = "OperatingSystemInfoType">
        <xs:attribute name = "MajorVersion" type = "xs:unsignedInt" use = "required"/>
        <xs:attribute name = "MinorVersion" type = "xs:unsignedInt" use = "required"/>
        <xs:attribute name = "BuildVersion" type = "xs:unsignedInt" use = "required"/>
      </xs:complexType>
      <xs:element name = "MsiInfo" type = "MsiInfoType"/>
      <xs:complexType name = "MsiInfoType">
        <xs:attribute name = "ProductCode" type = "xs:string" use = "required"/>
        <xs:attribute name = "Version" type = "xs:string" use = "optional"/>
        <xs:attribute name = "IsPerUser" type = "xs:boolean" use = "required"/>
      </xs:complexType>
    </xs:choice>
    <xs:element name = "ProductFamilyRef" type = "ProductFamilyRefType">

```



```
</xs:element>
</xs:sequence>
  xs:documentation>
```

This is product display name, for example,

—Windows XP

—Windows Vista

—Windows Server 2003

—Windows Server 2008

—2007 Office

```
</xs:documentation>
```

```
<xs:attribute name = "ID" type = "cgdcc-core:GUIDType">
```

```
</xs:attribute>
```

```
</xs:complexType>
```

```
</xs:sequence>
```

```
</xs:complexType>
```

```
</xs:schema>
```

附录 B

(资料性附录)

核心配置基线标记应用示例

B.1 “口令长度最小值为 8 位字符长度”核心配置基线 XML 示例

```

<? xml version = "1.0" encoding = "UTF-8"?>
<CGDCC—Package xmlns:admx = "http://schemas.microsoft.com/GroupPolicy/2008/03/PolicyDefinitions" xmlns:xsi = "http://www.w3.org/2001/XMLSchema-instance" xmlns:cgdcc-core = "http://schemas.sic.com/CGDCC/SecurityCompliance/core" xmlns = "http://schemas.sic.com/CGDCC/SecurityCompliance"
  <CGDCC-FormatInfo>
    <Version Minor = "0" Major = "1"/>
    <Description>此基线格式为 1.0 版本</Description>
  </CGDCC-FormatInfo>
  <CGDCC-Baseline Name = "CGDCC-Win7-sp1" ID = "{b5d9580f-7753-4dfb-9e53-634057e2a512}">
    <Version Minor = "0" Major = "1"/>
    <Mode = "Published"/>
    <VersionControl>
      <Publisher Name = SIC>
      </Publisher>
      <OriginalBaselineID>{71a71226-6325-41be-99dc-6af28cb617da}</OriginalBaselineID>
      <RevisionNumber>0</RevisionNumber>
    </VersionControl>
    <SettingGroup Name = "账户策略\口令管理" ID = "{d5a1fca2-3933-4dd0-9b88-1995ceb14611}"
      OriginalSettingGroupID = "{923ae966-e0c3-486c-b883-806cc9a188e2}">
      <Description>口令策略组包含的策略可控制这些口令管理策略:强口令、口令历史维护,以便阻止重复使用口令,并阻止重复使用可还原加密。
    </Description>
      <Version Minor = "0" Major = "1"/>
      <Setting Name = "口令长度最小值" ID = "{4b78f63c-fdae-42e8-b9f1-a161163a9c7f}">
      <Version Minor = "0" Major = "1"/>
      <Content>
      <Description>此策略设置确定用户账户密码包含的最少字符数。</Description>
      <SettingProductInfo>
        <UIPath>计算机配置\Windows 设置\安全设置\账户策略\密码策略</UIPath>
        <DefaultValue>0 characters</DefaultValue>
        <Vulnerability>密码攻击的类型包括字典式攻击(试图使用普通的词和词组)和蛮力攻击(尝试每一个可能的字符组合)。同样攻击者有时会试图获取账户数据库,这样他们就可以使用工具来发现账户和密码。</Vulnerability>
        <Countermeasure>配置“口令长度最小值”策略值为 8 或者更大。如果设置字符的数量为 0,

```

将不会需要口令。在大多数环境中,我们推荐8字符口令因为它足够长,可以提供足够的安全保障,同时让用户记住也不是太难。规定了口令的最小长度,就增加了非法用户破译口令的难度,防止其冒用登录。如果本地计算机口令长度最小值太小,攻击者可以轻松破译用户口令。

```

</Countermeasure>
<PotentialImpact>但口令长度最小值又不宜设置的太大,否则使用者须记忆很长的口令,容易忘记口令。</PotentialImpact>
<ValueRange High = "14" Low = "0">
<Unit>字符</Unit>
<ValueMappingTable>
  <Mapping FriendlyName = "Not Defined">
    <BehaviorDescription/>
    <DCMValue ValueA = "Not Defined"/>
    <GPOValue ValueA = "not defined"/>
  </Mapping>
  <Mapping FriendlyName = "Not Configured">
    <BehaviorDescription/>
    <DCMValue ValueA = "Not Configured"/>
    <GPOValue ValueA = "not configured"/>
  </Mapping>
  <Mapping FriendlyName = "Not Applicable">
    <BehaviorDescription/>
    <DCMValue ValueA = "Not Applicable"/>
    <GPOValue ValueA = "not applicable"/>
  </Mapping>
  <Mapping FriendlyName = "Not Recommended">
    <BehaviorDescription/>
    <DCMValue ValueA = "Not Recommended"/>
    <GPOValue ValueA = "not recommended"/>
  </Mapping>
  <Mapping FriendlyName = "Recommended">
    <BehaviorDescription/>
    <DCMValue ValueA = "Recommended"/>
    <GPOValue ValueA = "recommended"/>
  </Mapping>
</ValueMappingTable>
</Content>
<SettingDiscoveryInfo Scope = "Machine" DiscoveryType = "WMI">
  <WMIDiscoveryInfo>
    <cgdcc-core;Namespace>root\rsop\computer</cgdcc-core;Namespace>
    <cgdcc-core;Class>RSOP_SecuritySettingNumeric</cgdcc-core;Class>
    <cgdcc-core;Property>Setting</cgdcc-core;Property>
    <cgdcc-core;Where>KeyName = 'MinimumPasswordLength' And precedence = 1</cgdcc-core;Where>
  </WMIDiscoveryInfo>
</SettingDiscoveryInfo>

```



```

</WMIDiscoveryInfo>
</SettingDiscoveryInfo>
<DataType>Int64</DataType>
<ExportInfo GPOGenerateFormat = "INF">
  <Inf Name = "MinimumPasswordLength" SectionName = "System Access" DataType = "REG_
    DWO-RD"/>
</ExportInfo>
</Setting>
<Check>
  <SettingRef setting_ref = "{4b78f63c-fdae-42e8-b9f1-a161163a9c7f}"/>
  <ExistentialRule Name = "Minimum password length" ValueA = "0" Operator = "GreaterThan" Se-
    verity = "Informational">
  </ExistentialRule>
  <ValidationRules> <SettingRule Name = "Minimum password length" Operator = "Great-
    erEquals" Severity = "Informational">
    <Value ValueA = "8"/>
  </SettingRule>
</ValidationRules>
</Check>
</CGDCC-Baseline>
<Product ID = "{1739795a-9a4f-4032-b8db-8834dba5a0eb}" DisplayName = "Windows 7">
  <OperatingSystemInfo BuildVersion = "7601" MinorVersion = "1" MajorVersion = "6"/>
</CGDCC-Package>

```

B.2 “口令长度最小值为 8 位字符长度”核心配置基线 XML 示例简要说明

【产品名称】Windows7 操作系统 6.1 7601

【配置项标识】:4b78f63c-fdae-42e8-b9f1-a161163a9c7

【配置项名称】:口令长度最小值

【配置项描述】:此配置确定账户口令包含的最少字符数。0 代表无密码设置。

【配置类型】:WMI 配置

【配置项组别】:账户策略/口令管理

【取值范围】:0—24 位字符

【配置项基值】:8 位字符

【赋值路径】:计算机配置\Windows 设置\安全设置\账户策略\密码策略

【检查规则】:大于或等于

附录 C
(资料性附录)
核心配置基线应用示例

按照 GB/T 30278—2013 第 9 章要求,针对大规模计算机终端的自动化安全配置管理,需配备核心配置自动化部署及监测平台。该平台由配置编辑、配置验证、配置部署和配置监测四种基本工具构成,分别支持核心配置基线的编辑、验证、部署和状态监测等四个应用环节,如图 C.1 所示。本附录以终端核心配置管理系统(CGDCC)为例,说明核心配置基线的具体应用流程。

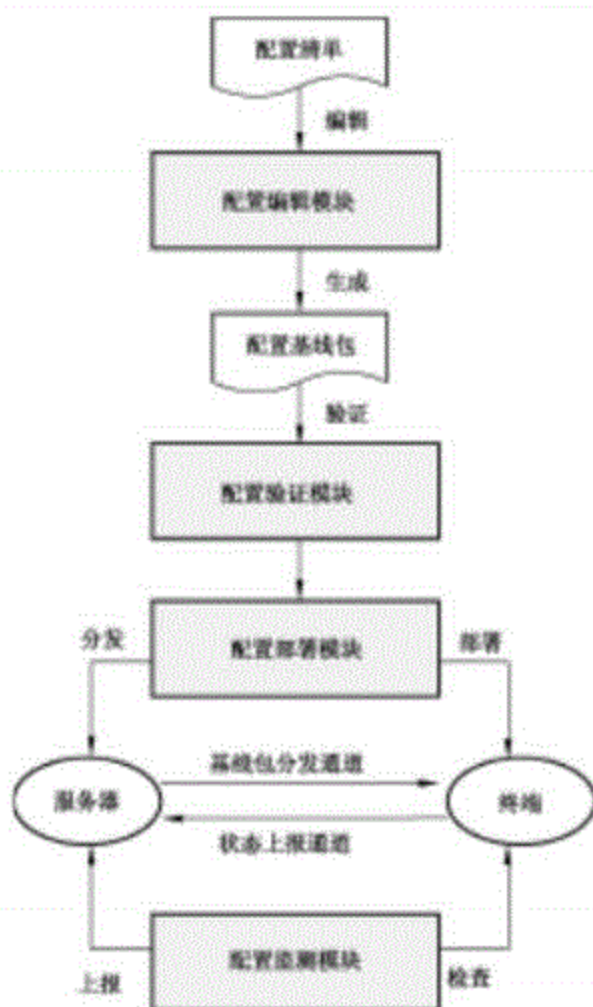


图 C.1 核心配置基线应用流程

C.1 核心配置编辑

核心配置编辑模块提供图形化的配置基线信息录入界面,可实现自动生成符合本标准规定的基线结构和标记规则(见第 6 章)的核心配置基线。用户可根据安全要求通过该功能对核心配置基线中的配置项及其赋值进行修改。基线编辑模块主界面如图 C.2 所示。



图 C.2 核心配置基线编辑模块主界面

该模块生成核心配置基线的操作过程如下：

a) 录入基线基本信息

选择新建基线,并输入适用产品名称、描述、备注等基本信息,如图 C.3 所示。

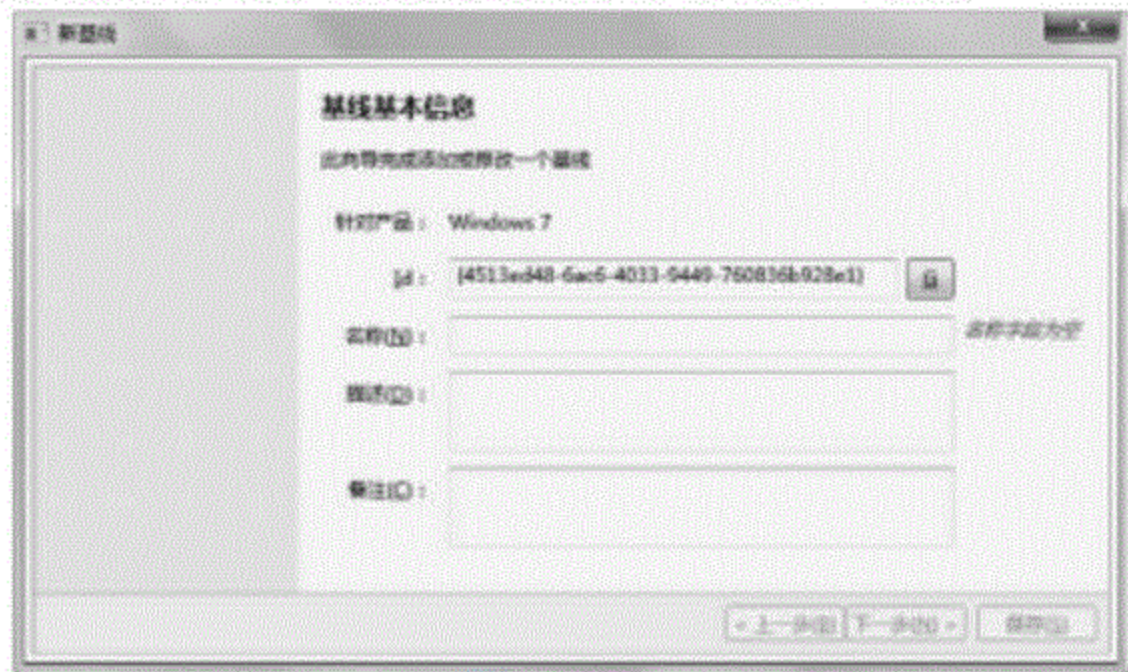


图 C.3 基线基本信息编辑界面

b) 添加基线的配置组

在基线基本信息录入完成后,进入基线配置组的添加或删除操作,如题 C.4 所示。



图 C.4 基线配置组编辑界面

c) 编辑基线的配置项

可选择某个配置组进行配置项的添加、删除及编辑修改操作,如图 C.5 所示。



图 C.5 配置项编辑界面

d) 自动生成基线

确认基线信息并保存后,工具自动生成一条新的核心配置基线(*.cab)。

C.2 核心配置验证

配置验证模块对生成的核心配置基线自动进行有效性、适用性和兼容性测试,保证基线配置项的赋值合理有效,配置项之间不存在冲突,不会对终端应用环境造成不良影响。技术人员可根据基线验证结果,对有问题的配置基线进行编辑修改。基线验证模块主界面如图 C.6 所示。

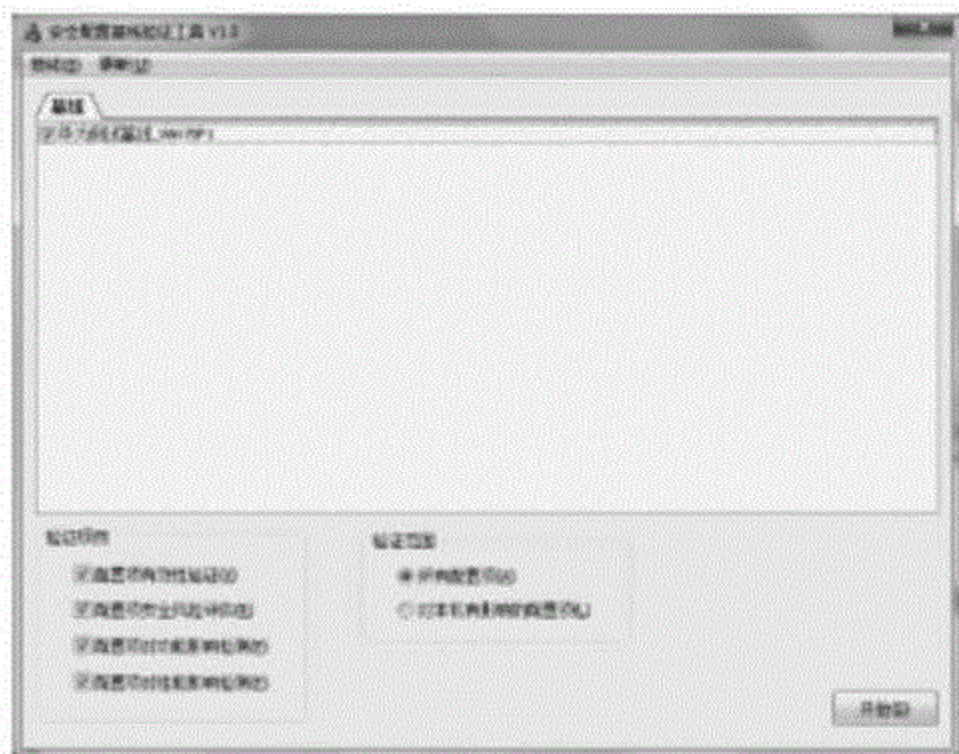


图 C.6 核心配置基线编辑模块主界面

该模块验证核心配置基线的操作过程如下:

a) 导入待验证的基线

在基线验证模块主界面的菜单中选择“基线”、“添加”进入基线添加界面,选择新生成好的基线 (*.cab)导入工具中即可。如图 C.7 所示:

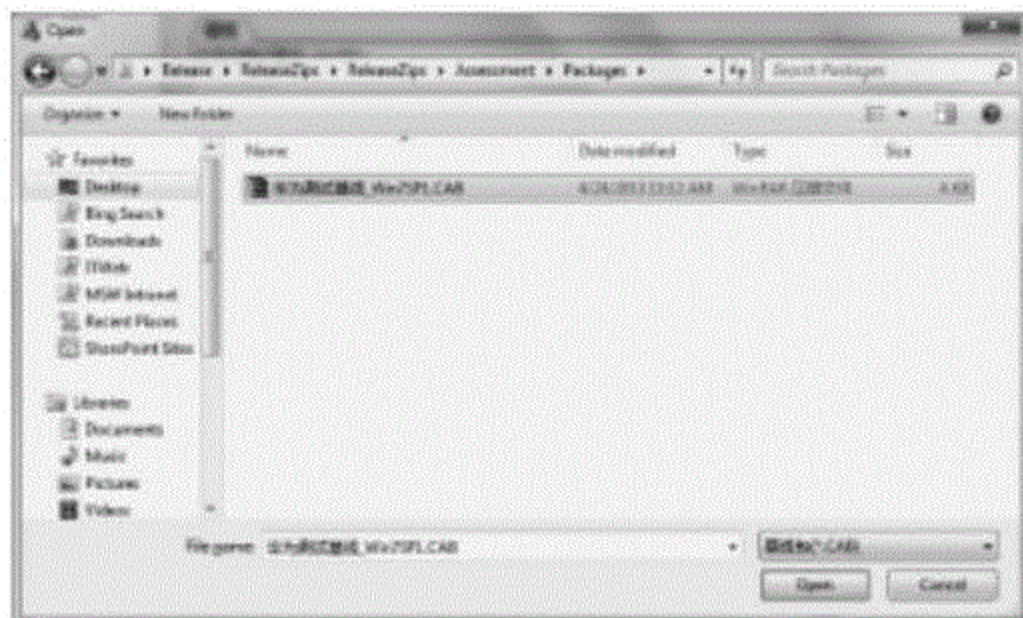


图 C.7 基线验证导入操作

b) 验证核心配置基线

在主界面“基线列表栏”勾选需要验证的基线,并选择验证项目和验证范围。勾选完毕后,点击“开始”按钮进行验证。

c) 显示验证结果

验证完成后进入验证结果界面,其中会详细列出未通过的项目及其原因,如图 C.8 所示。

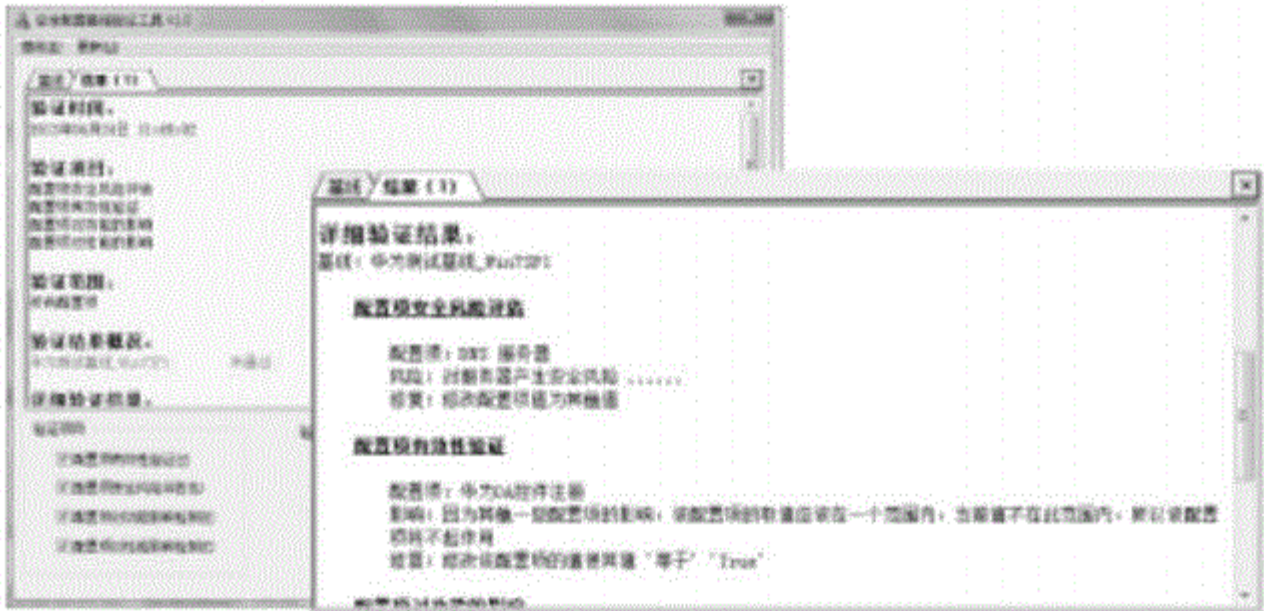


图 C.8 验证结果显示

C.3 核心配置部署

配置部署模块将核心配置基线分发至指定的计算机终端进行部署。终端上的配置执行工具对基线进行自动解析,并根据配置项基值和赋值路径逐项进行参数设置。为保证基线在网络中传输的安全性,可采取基线加密或传输加密机制。基线管理主界面如图 C.9 所示。



图 C.9 基线管理界面

该模块部署核心配置基线的操作过程如下:

a) 上载基线

在基线管理界面上方工具栏中选择“基线上载”,进入上载基线向导流程。选择“要上载的基线后”,

点击“开始上载”，并完成。如图 C.10 所示。



图 C.10 基线上载向导界面

b) 部署基线

在基线管理界面上方工具栏中选择“基线部署”，进入指派基线向导流程。经过选择基线、选择部门/IP段、制定循环检测时间、确认指派信息等环节，最终完成基线自动化部署，如图 C.11 所示。

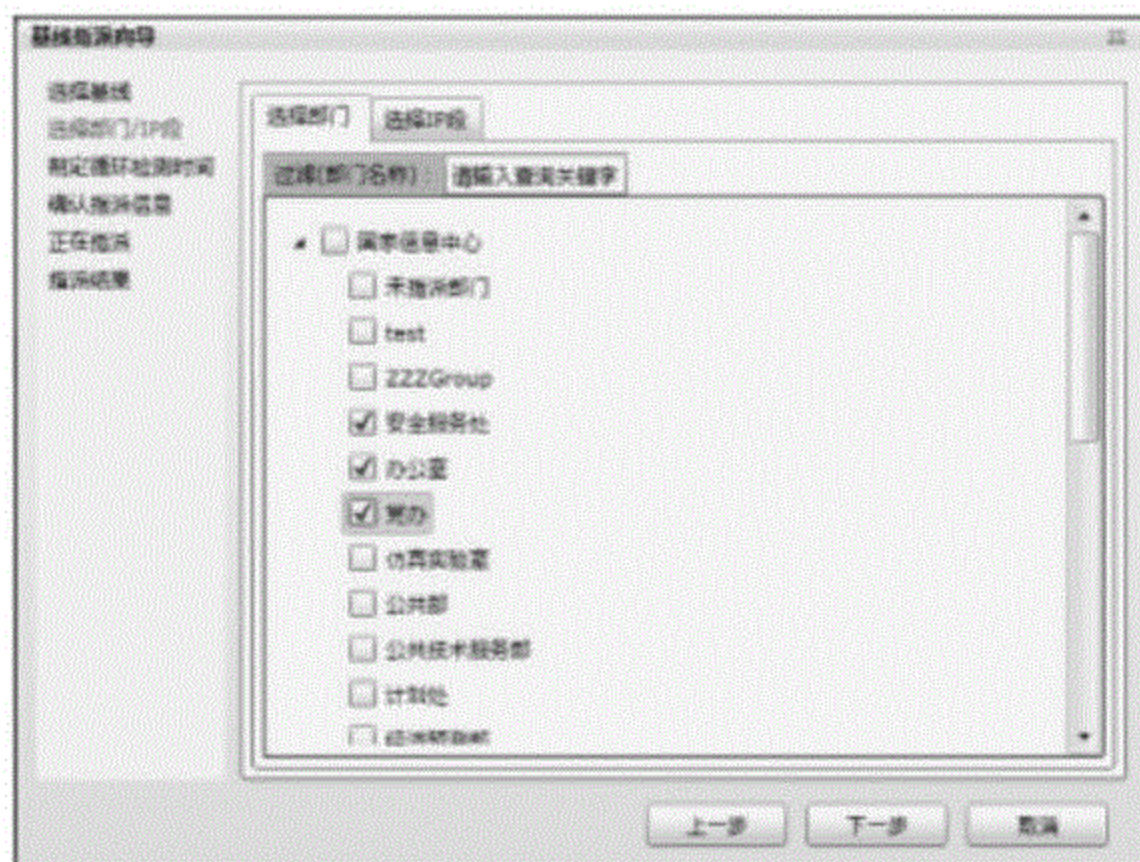


图 C.11 基线部署向导界面

C.4 核心配置监测

配置监测模块自动检查计算机终端安全配置基线的合规性,将检查结果上报服务端进行统计分析,并以图表形式进行展示。全网终端安全配置状态监测情况和配置策略达标情况分别如图 C.12 和图 C.13 所示。



图 C.12 全网终端安全配置状态监测情况

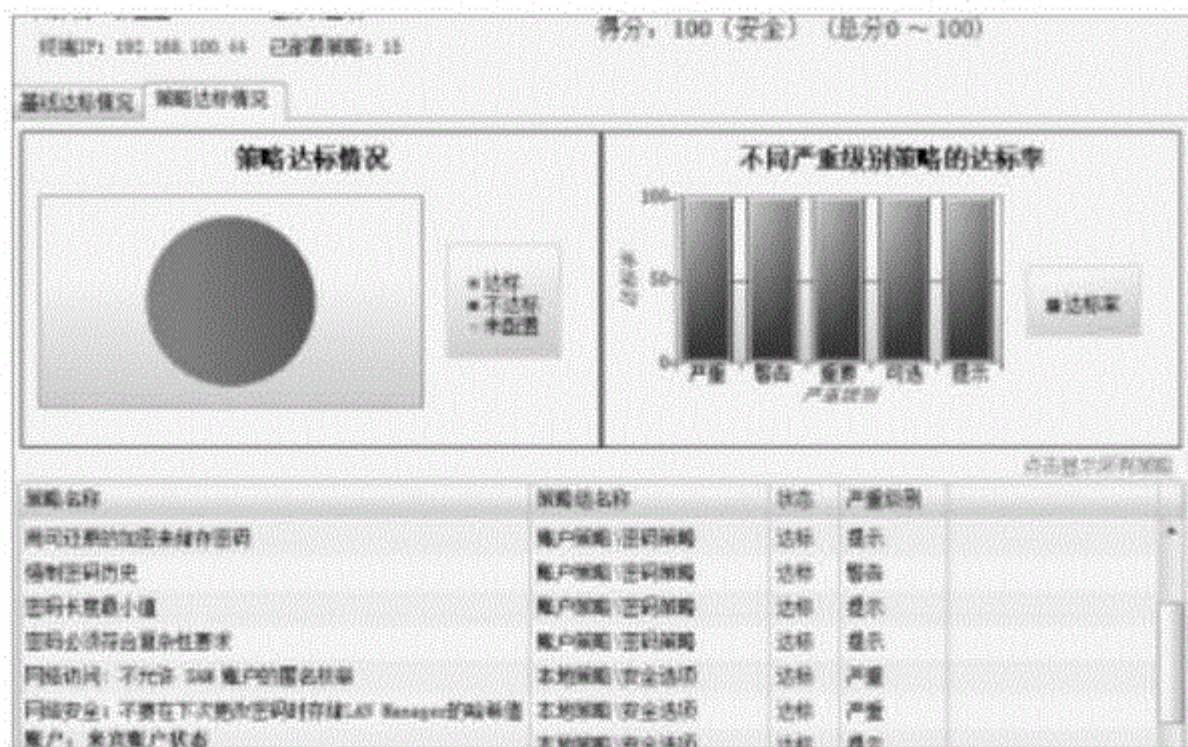


图 C.13 终端配置策略达标情况

参 考 文 献

- [1] GB/T 19667.1—2005 基于 XML 的电子公文格式规范 第 1 部分:总则
 - [2] GB/T 30278—2013 信息安全技术 政务计算机终端核心配置规范
-

