GJB

中华人民共和国国家军用标准

FL 0112 GJB 7554—2012

网络安全设备管理接口要求

Requirements for interface of network security device management

2012—07—24 发布 2012—09—01 实施

中国人民解放军总装备部 批 准

目　次

前　言

本标准附录A和附录B是规范性附录，附录C是资料性附录。

本标准由总参信息化部提出。

本标准起草单位：总参第六十一研究所、空军装备研究院通信导航与指挥自动化研究所、上海安纵信息科技有限公司。

本标准主要起草人：李京鹏、韩明畅、王　博、唐　鑫、张增军、郁　朗、刘　羽、包　伟、郑　勇。

网络安全设备管理接口要求

1 范围

本标准规定了军队计算机网络中的安全设备和安全管理系统之间的接口，以及安全设备的人机接口。

本标准适用于军队计算机网络中的安全设备和安全管理系统的研制和采购。

2 引用文件

下列文件中的有关条款通过引用而成为本部分的条款。凡注日期或版次的引用文件，其后的任何修改单(不包括勘误的内容)或修订版本都不适用于本部分，但提倡使用本部分的各方探讨使用其最新版本的可能性。凡未注日期或版次的引用文件，其最新版适用于本部分。

GB 2312－1980 信息交换用汉字编码字符集基本集

ISO/IEC 14882－2003 程序设计语言 C＋＋ 2003.10 ISO

IETF RFC1769 简单网络时间协议 1995.3 IETF

IETF RFC2246 传输层安全协议(TLS)版本 1.0 1999.1 IETF

IETF RFC2459 互联网络 X.509 公钥基础设施证书与证书撤销列表(CRL)概述 1999.1 IETF

IETF RFC4765 入侵检测消息交换格式 2007.3 IETF

3 术语、定义和缩略语

下列术语定义和缩略语适用于本标准。

3.1 术语定义

3.1.1 安全设备 security device

为保障目标网络的安全而引入的软硬件系统(或者设备)。

3.1.2 安全管理系统 security management system

对安全设备实施管理的软硬件系统。

3.1.3 安全策略 security policy

安全设备实现安全功能需要的一系列参数和规则。安全策略由参与安全管理的人员依据相关的法规、政策、要求、规定、规范、命令及实际安全需求制定和配置。

3.1.4 安全事件 security event

由安全设备产生，反映网络和系统安全状态变化的信息，包括各种网络安全设备产生的告警、审计日志、设备状态信息等。

3.1.5 系统接口 system interface

安全管理系统与安全设备之间的信息交换接口。符合系统接口要求的安全管理系统能够通过系统接口，实施对符合系统接口要求的安全设备进行管理。

3.1.6 用户接口 user interface

安全管理系统与参与安全管理的各类人员之间的人机接口。通过用户接口，参与安全管理的各类人员能够使用安全管理系统完成相关的管理操作。

3.1.7 管理代理 management agent

驻留在被管理安全设备中的可执行软件模块。安全管理系统能够通过管理代理与安全设备交互，实现对安全设备的管理控制。

3.1.8 状态视图 status view

安全设备上一系列能反映设备的状态、功能、性能等信息的组合，以 XML 文档的形式进行展示、保存和描述。

3.1.9 参数封包 Parameters Envelop Package

包含特定格式和内容的 XML 文档，用作接口方法的参数或返回值。

3.2 缩略语

API——应用编程接口 Application Programing Interface；
ASN.1——抽象语法定义 1 Abstract Syntax Notation One；
B/S——浏览器/服务器 Browser/Server；
C/S——客户端/服务器 Client/Server；
CPU——中央处理单元 Central Processing Unit；
DTD——文档类型定义 Document Type Definition；
FTP——文件传输协议 File Transfer Protocol；
GIF——可交换图形文件格式 Graphics Interchange Format；
HTTP——超文本传输协议 Hypertext Transfer Protocol；
IC 卡——集成电路卡或智能卡 Integrated Circuit Card；
ID——身份或标识符 Identification；
IDMEF——入侵检测消息交换格式 Intrusion Detection Message Exchange Format；
IMAP——Internet 消息访问协议 Internet Message Access Protocol；
IP——互联网络协议 Internet Protocol；
JPEG——联合图像专家组压缩文件格式 Joint Photographic Expert Group；
LOGO——标记、标志；
MAC——介质访问控制 Media Access Control；
NAT——网络地址转换 Network Address Translation；
NNTP——网络新闻传输协议 Network News Transfer Protocol；
NTP——网络时间协议 Network Time Protocol；
SMB——服务器信息块 Server Message Block；
SMTP——简单邮件传输协议 Simple Message Transfer Protocol；
SNMP——简单网络管理协议 Simple Network Management Protocol；
SSH——安全 Shell Security Shell；
SSL/TLS——安全 Socket 层/传输层安全 Security Socket Layer/Transfer Security Layer；
TCP——传输控制协议 Transfer Control Protocol；
TXT——纯文本文件格式 Text；
UDP——用户数据报协议 User Datagram Protocol；
URL——统一资源定位 Uniform Resource Locator；
USB——通用串行总线 Universal Serial Bus；
USBKEY——一种 USB 接口的智能外设，用于存储用户证书，完成签名和加密算法；
VPN——虚拟专网 Virtual Private Network；
XML——可扩展标记语言 Extensible Markup Language。

4 系统接口要求

4.1 系统接口方式

4.1.1 接口方式选择

系统接口方式是指系统接口的定义和实现方法。

可选的系统接口方式有协议通信和代理嵌入两种方式。

具备独立设备形态的安全设备通常选择协议通信方式实现系统接口；不具备独立设备形态的安全设备通常选择代理嵌入方式实现系统接口。

4.1.2 协议通信方式

通过采用通用的协议或定义专用管理通信协议的方式实现系统接口。

采用这种方式实现的系统接口至少应做出如下定义：

a) 使用的下层通信协议，例如：TCP、UDP、IP，甚至更低层的通信协议；

b) 命令、命令参数及数据的语法、语义和编码方式；

c) 服务器端及客户端的状态迁移过程；

d) 安全机制；

e) 差错控制机制。

接口定义应根据具体实现采用 XML、ASN.1 或正则表达式(TXT)等方式给出。

4.1.3 代理嵌入方式

通过在被管理对象上嵌入管理代理的方式实现系统接口。

采用这种方式实现的系统接口至少应做出如下定义：

a) 管理代理的目标运行环境和运行条件；

b) 接口参数及数据的语法、语义和编码方式；

c) 管理代理自身及管理代理交互对象的状态迁移过程；

d) 安全机制；

e) 差错控制机制。

接口定义应根据具体实现封装成 API 并提供详细的手册及调试试验环境。

4.2 安全策略管理

安全策略的管理应符合如下要求：

a) 安全策略在安全管理系统生成，并以本标准规定的格式以协议通信或代理嵌入的方式发送给安全设备；

b) 安全设备接收到安全策略时，应对该安全策略进行校验并立即执行，并将执行结果返回给安全管理系统；

c) 当安全策略执行失败时，安全设备应能恢复到执行前的状态；

d) 安全设备应能够向安全管理系统提供当前正在执行的安全策略。

采用代理嵌入方式实现安全策略管理见附录 A 中 A.1.2.5 和 A.3.3。

4.3 安全事件管理

安全设备应将检测到的安全事件和记录的日志发送到安全管理系统；安全管理系统应能够对接收到的安全事件和日志进行存储、显示和告警等处理。

采用代理嵌入方式实现安全事件管理见附录 A 中 A.1.2.5 和 A.4。

4.4 设备状态与性能监视

4.4.1 设备状态的查询

安全设备应在安全管理系统对其进行状态查询时将指定的状态信息反馈给安全管理系统。

采用代理嵌入方式实现设备状态查询见附录 A 中 A.1.2.5 和 A.3.4。

4.4.2 设备参数的配置

安全管理系统可以查询安全设备的基本设备参数，并对其进行修改设置；安全设备必须根据安全管理系统设定的参数进行相应的配置调整。

采用代理嵌入方式实现设备参数配置见附录 A 中 A.1.2.5 和 A.3.2。

4.5 维护性操作接口

维护性操作接口应至少能完成如下功能：

a） 时间设定，设定安全设备的当前时间；

b） 关机/重启，将安全设备关机或重新启动；

c） 手动升级，为安全设备进行升级操作；

d） 保存配置，通知安全设备保存当前的所有配置和安全策略；

e） 差错控制，对管理操作中发生的异常进行通报；

f） 查询操作，查询安全设备的管理信息。

采用代理嵌入方式实现维护性操作接口见附录 A 中 A.1.2.5 和 A.3.5。

4.6 系统接口安全

系统接口至少应具备以下安全机制：

a） 基于军队安全认证体系的安全设备和安全管理系统之间的双向鉴别验证；

b） 各种管理信息交换时的完整性、机密性、抗重放攻击能力和抗拒绝服务攻击能力；

c） 各种管理操作的授权控制、安全审计和不可否认性；

d） 各种安全策略的安全性。

采用代理嵌入方式实现系统接口安全见附录 A 中 A.1.2.5 和 A.1.4。

5 用户接口要求

5.1 基本要求

5.1.1 易用性

易用性要求如下：

a） 主界面按功能划分区域块；

b） 控件文字命名应该明确指示功能，用词准确，与其他控件名称易于区分；

c） 弹出窗口层次要少，最多不超过四层(不包括信息提示窗口)，软件功能尽量显示在主窗口上；

d） 常用按钮要支持快捷方式；

e） 界面元素标注要简洁、准确、规范，无歧意；

f） 完成相同或相近功能的按钮用组合框框起来，并要有功能说明或标题；

g） 界面要支持键盘自动浏览按钮功能，即 Tab 键的自动切换，Tab 键的顺序与控件排列顺序要一致，总体遵守从上到下，从左到右的顺序；

h） 界面上首先应输入的和重要信息的控件在 Tab 键自动切换的响应顺序中应靠前，位置也应放在窗口上较醒目的位置；

i） 默认按钮要支持回车选定，按回车后自动执行默认按钮对应操作；

j） 可写控件检测到非法输入后应给出说明并自动获得焦点；

k） 选项框按照选择几率的高低先后排列，并要有默认选项，支持 Tab 键切换选择；

l） 专业性强的页面要使用相关的专业术语，通用性页面要求使用通用性词汇；

m） 工具栏中的每一个按钮要有即时提示信息，工具栏的长度最长不能超出屏幕宽度，工具栏的图标能直观代表要完成的操作；

n） 状态条显示用户切实需要的信息，常用的有：当前操作、系统状态、用户位置、用户信息、提示信息、错误信息，当系统处理时间超过 3s 时，要使用进度条提示；

o） 界面缩放时，整体界面及其内容不能出现扭曲、变形的现象。

5.1.2 规范性

规范性要求如下：

a） 界面包含“菜单条、工具栏、状态栏、滚动条、右键快捷菜单”等标准元素。

b) 不允许操作的菜单、控件等要隐藏或禁用。

c) 按钮或菜单的文字如果为动词与名词的组合，则采用“动词＋名词”的形式，例如：“绘制表格”。

d) 如果启动和初始化软件需要花费较多的时间，则显示软件封面。该封面位于屏幕正中，大小为(400×300)像素，选用反映本软件特点的图片，同时包含文字说明。文字说明的内容应包含软件名称、版本号、发布时间、开发单位。如果启动或初始化时间超过 3s，在封面底部显示启动和初始化的进度条。

e) 使用系统标准正规的字体，中文采用标准字体“宋体”，英文采用标准字体 Times New Roman，需要艺术处理或有特殊要求的地方除外。

f) 同一单位的军用系列产品要保持一致的界面风格，背景色、字体、菜单排列方式、图标、安装过程、按钮用语等应该大体一致。

5.1.3 合理性

合理性要求如下：

a) 重要的命令按钮与使用较频繁的按钮放在屏幕对角线相交位置的正上方 1/4 处；

b) 对可能造成数据无法恢复的操作必须提供确认信息，给用户放弃选择的机会；

c) 专业术语与用户现有的业务用语一致；

d) 界面中的说明性文字全部使用简体中文；

e) 当使用多文档窗口时，父窗体或主窗体的中心位置应该在对角线焦点附近，子窗体位置应该在主窗体的左上角或正中，多个子窗体弹出时应依次向右下方偏移，能够显示各窗体的标题；

f) 错误使用容易引起界面退出或关闭的按钮不应该放在易点位置(横排开头或最后与竖排最后为易点位置)；

g) 非法的输入或操作应有详细明确的提示说明；

h) 对运行过程中出现问题而引起错误的地方要有提示，让用户明白错误出处，避免用户无限期的等待；

i) 提示、警告或错误信息用中文说明，说明内容应该清楚、明了、恰当。

5.1.4 美观与协调性

美观与协调性要求如下：

a) 长宽比或宽长比接近黄金点比例(0.618)；

b) 布局要合理，不能过于密集，也不能过于空旷，合理利用空间；

c) 相邻或同组的按钮大小相同；

d) 按钮的大小与界面的大小和空间要协调；

e) 不能在空旷的界面上放置很大的按钮；

f) 放置完控件后界面不应有很大的空缺位置；

g) 字号大小要与界面的大小比例协调；

h) 界面色调要柔和，具有亲和力，避免使用刺目的颜色；

i) 界面风格要保持一致，有标准的图标设计风格，统一的构图布局，统一的色调、对比度、色阶，以及图片风格；

j) Web 界面底图应该使用浅色，低对比，不能使用过多颜色。

5.1.5 菜单实用性

菜单实用性要求如下：

a) 菜单位置按照 5.3.1.2 执行；

b) 菜单采用“常用－主要－次要－工具－帮助”的位置排列；

c) 菜单要根据菜单选项的含义进行分组，并按照一定的规则进行排列，必要时用横线隔开；

d） 一组菜单的使用有先后要求或有向导作用时，应该按先后次序排列；
e） 没有顺序要求的菜单项按使用频率和重要性排列，常用的放在开头，不常用的靠后放置；重要的放在开头，次要的放在后边；
f） 菜单深度最多控制在三层以内；
g） 常用的菜单要有相应加速按钮；
h） 对与进行操作无关的菜单要用屏蔽的方式加以处理，或采用动态加载方式，即只有需要的菜单才显示；
i） 菜单前的图标能直观代表要完成的操作，不宜太大，与字高保持一致；
j） 主菜单的宽度要接近，字数不应多于四个，每个菜单的字数尽量相同；
k） 主菜单数目不应太多。

5.1.6 使用安全性

使用安全性要求如下：

a） 排除可能会使应用非正常中止的错误；
b） 对用户输入数据的有效性进行检验；
c） 采用相关控件限制用户输入值的种类；
d） 当只允许用户选择一个选项时，采用单选框；当选择的可能性较多时，采用复选框；当选项特别多时，可以采用列表框或下拉式列表框；
e） 避免用户做未经授权或没有意义的操作；
f） 对可能引起致命错误或系统出错的输入字符或动作要加限制、屏蔽和处理；
g） 对可能发生严重后果的操作要有补救措施，通过补救措施用户可以回到原来的正确状态；
h） 对一些特殊符号的输入、与系统使用的符号相冲突的字符等要进行判断并阻止用户输入该字符；
i） 在输入有效性字符之前应该阻止用户进行只有输入之后才可进行的操作；
j） 在读入用户所输入的信息时，根据需要选择是否去掉前后空格。

5.2 远程管理界面方式

网络安全设备的远程管理界面可以使用 B/S 结构，采用 Web 页面作为界面；也可以使用 C/S 结构，采用专用的管理程序进行管理配置。此接口要求不限定使用其中任何一种方式或两种方式的结合，但是推荐使用 B/S 方式。另外，对于远程管理的设备，还需要提供基于命令行方式的管理，以提供基本配置管理和灾难恢复功能。

5.3 界面元素

5.3.1 界面布局

5.3.1.1 登录界面

用户登录界面如图 1 所示。

界面元素包括：

a） 军队标识：经过美工设计的军徽图案；
b） 产品 LOGO：产品名称(军用 XXX)和产品型号，以图片方式提供；
c） 管理员帐号输入框：用字符明码显示；
d） 口令输入框：口令字符一律显示为星号“*”；
e） 操作按钮：“确定”、“关闭”；
f） 指纹认证：显示用户输入的指纹图案；
g） 认证提示信息：显示指纹认证成功与否的信息；
h） 厂家名称，支持电话：显示研发此产品的厂家名称和技术支持电话；
i） 背景图：反映本产品特点的图片。

登录界面应以全屏显示，界面元素内容和布放位置参考以上示意图，以美观实用为设计目标。若系统支持指纹认证，则在界面上显示“指纹认证”和“认证提示信息”组件。另外，此界面还应支持认证系统，当用户提供正确的证书时也应能够登录。

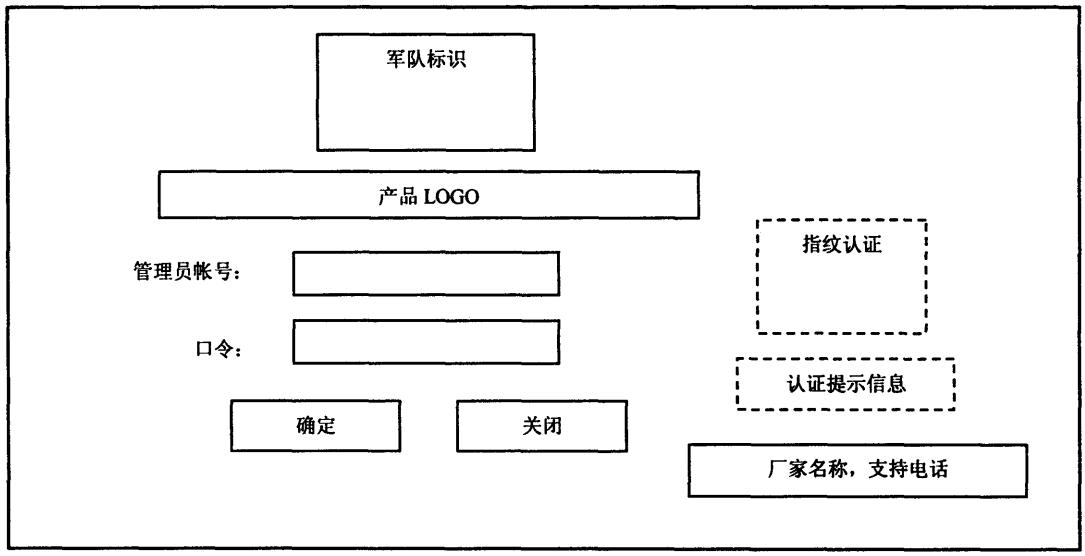

图 1　WEB 登录界面示意图

5.3.1.2　管理主界面

5.3.1.2.1　B/S 形式

5.3.1.2.1.1　界面布局与界面元素

B/S 形式的管理 Web 页面布局分为四个框架，分别为系统标识区，加速按钮区、功能控制区与功能显示区，其窗体布局如图 2 所示。

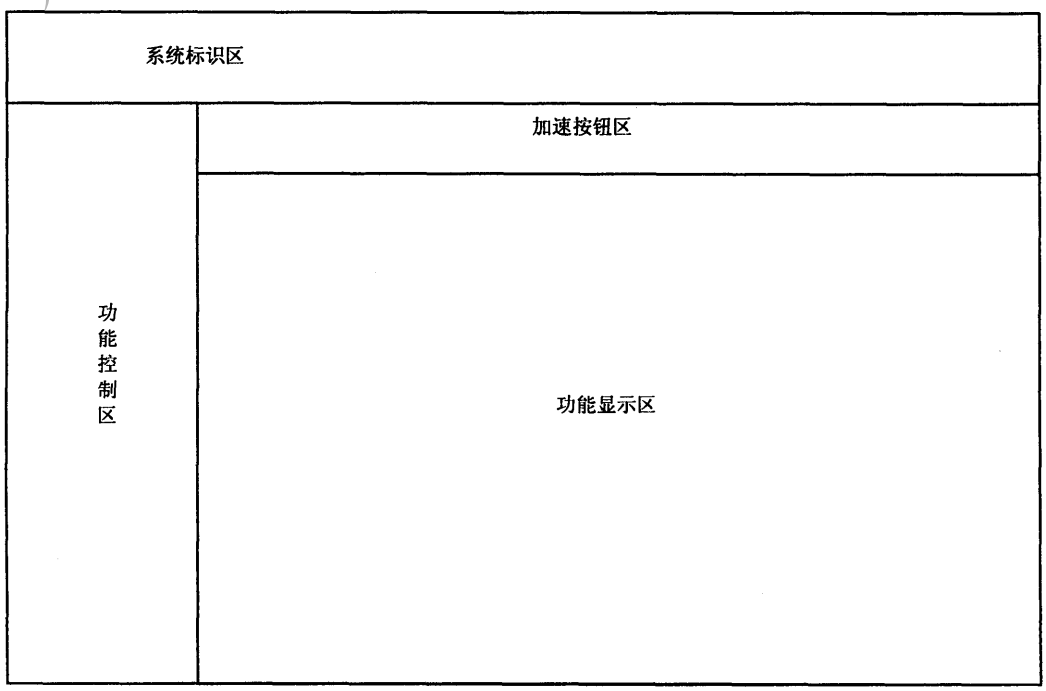

图 2　Web 形式管理主界面设计图

界面元素包括：

a)　系统标识区：用整幅图片填充，内容包括军队标识、产品 LOGO 等，同一公司的产品采用统

一背景的图片，颜色、字体、尺寸等属性；

b) 加速按钮区：放置常用的功能加速按钮，如保存、安全策略导入导出等，加速按钮的图标要能清晰明了地指示将要执行的操作；

c) 功能控制区：显示 Web 树形的导航菜单，与功能显示区关联，具体内容见附录 B；

d) 功能显示区：显示左侧功能控制选项所指示的内容，整体页面布局应整齐有序。

5.3.1.2.1.2 **系统实现要求**

采用 B/S 形式的人机界面时，系统实现应满足以下要求：

a) 如果一套管理系统同时提供 B/S 方式和 C/S 方式的管理界面，则两种模式下用户界面的外观风格和界面组织方式大致相同。

b) 页面应支持 800×600、1024×768、1280×960 等多种分辨率和 16 位、32 位色阶。最佳显示效果为 1024×768，色阶为 32 位色。

c) 对流行的浏览器兼容，重点支持 Internet Explorer 浏览器(6.0 或以上版本)。

d) 页面中所有用到的图片文件均采用 JPEG 或 GIF 格式。

e) 页面层级不宜过深，建议不超过四层。

f) 如果页面层级在三层或以上，则应以导航条明确标注页面层次和当前位置。标注方式形如：“首页>>二级页面名称>>三级页面名称>>……>>当前页面名称”，每个页面名称都具有链接属性。

g) 每个页面都要定义简明准确的标题，不允许出现“New Page”或“Untitled Document”的字样；

h) 在页面中尽量少使用滚动条，不宜使用横向滚动条。

i) 对于有超级链接的文字采用蓝色，鼠标悬停时加下划线。

5.3.1.2.2 **C/S 形式**

5.3.1.2.2.1 **界面布局与界面元素**

C/S 风格的界面要求采用资源管理器风格，如图 3 所示。该界面分为六个区域，分别是菜单栏、常用功能加速按钮区、功能控制区、功能显示区、实时信息显示区(可选)、状态栏。

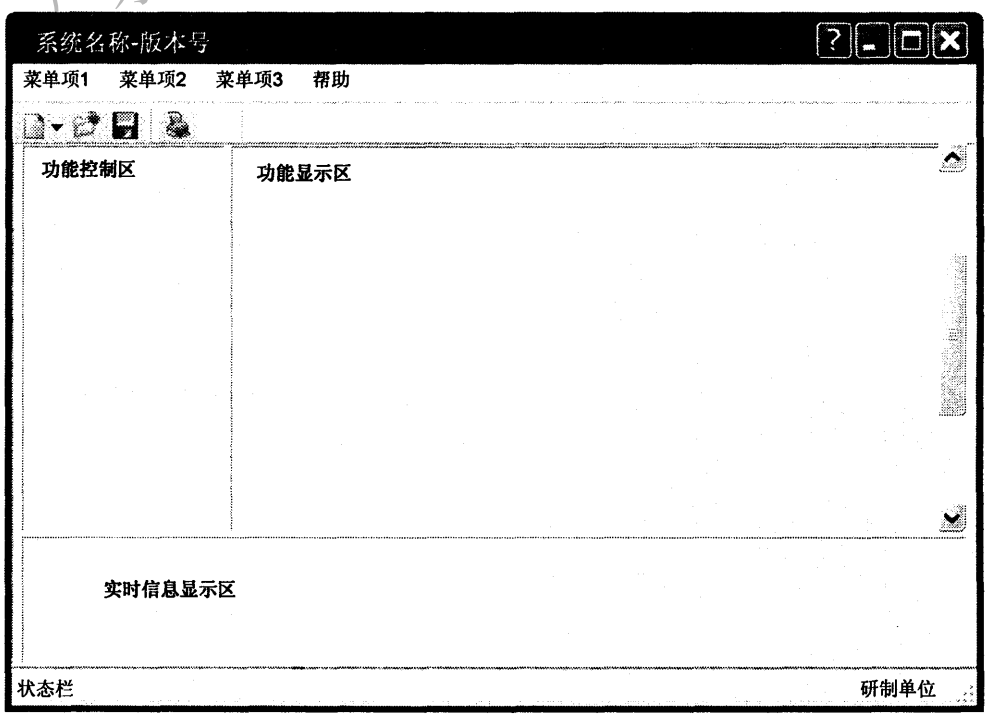

图 3 C/S 界面设计图

窗口标题格式按“系统名称—版本号”的格式给出，窗体右下角显示研制单位名称，窗体六个区域分别显示以下内容：

a） 菜单栏：按功能依次放置菜单项；

b） 常用功能加速按钮区：放置常用的功能加速按钮，可根据需要进行增减；

c） 功能控制区：放置树形控制组件，与功能显示区关联；

d） 功能显示区：显示左侧功能控制选项所指示的内容；

e） 实时信息显示区(可选)：显示程序动态捕获的实时信息，如系统资源、网络流量、信息统计等信息；

f） 状态栏：显示当前系统状态，如当前按钮名称、菜单快捷键、当前系统操作等。

5.3.1.2.2.2 系统实现要求

采用 C/S 形式的人机界面实现时，系统实现应满足以下要求：

a） 软件启动后，主窗口要充满用户的可见显示窗口。

b） 窗口标题栏左侧包含产品图标，该图标规格统一为(16×16)像素，能体现软件的功能，可以加入 1～2 个反映软件特点的关键汉字。

c） 如果主窗口的内容框中含有较多的图形组件，可利用分隔框将窗口划分为独立的面板，进行规划布局。使用分隔框时：

1） 分隔框数量不宜过多，一个窗口中最多允许同时存在三个独立的分隔框；

2） 所有分隔框可通过拖拽的方式改变尺寸；

3） 用户可以选择显示/隐藏各个分隔框；

4） 如果一个分隔框内所显示的内容超过分隔框大小，应生成滚动条；

5） 分隔框初始的布局方式可选择图 4 所示的任意一种。

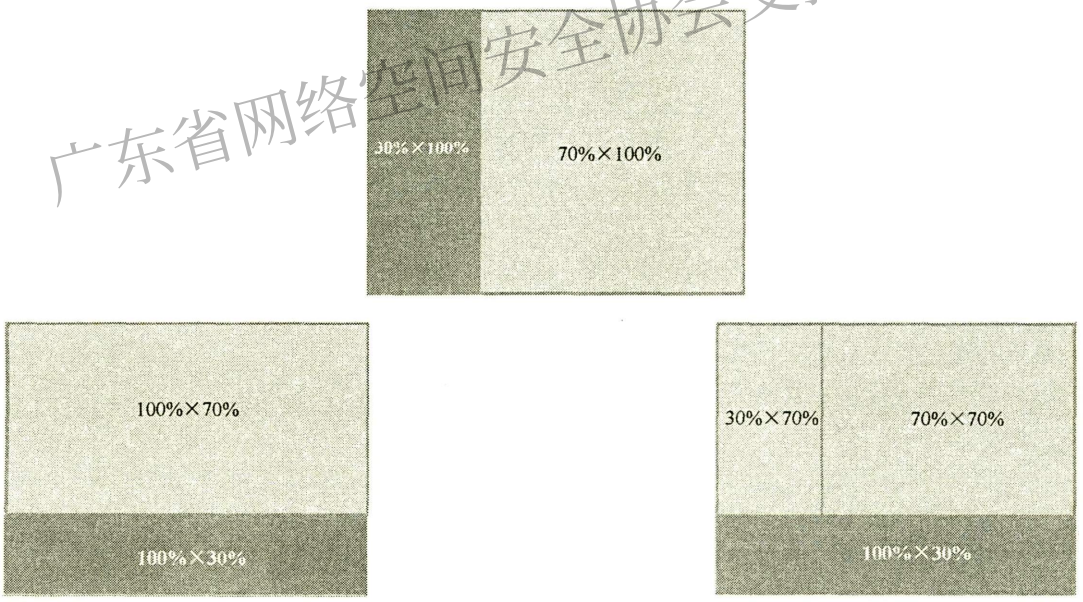

图 4 三种可选的分隔框布局方式

d） 主窗口包含标题栏、菜单栏、工具栏、状态栏、用户区和可调边界，其中标题栏上有窗口菜单按钮、最小化按钮、最大化按钮、关闭按钮等内容。

e） 标题栏上应能显示软件名称及打开文件名(若有)，例如：标题栏上可以显示“XXXX 软件－YYY”，其中“YYY”表示打开的文件名，如果没有打开的文件，则只显示软件名称和版本号即可。

f） 除主窗口外，其他窗口标题前均不加图标。

g） 子窗体位置在主窗体的左上角或正中，初始大小不覆盖父窗体。

h） 多个子窗体弹出时依次向右下方偏移，能够显示各窗体标题。

5.3.2 菜单

菜单要求如下：

a) 主菜单始终被显示，不设置任何可以关闭菜单栏的选项。

b) 菜单栏不允许包含多行。

c) 任何一个独立进程的窗口中都可以含有菜单栏，对话框不含菜单栏。

d) 顶级菜单项仅用文本描述，不使用图标，子菜单项可以使用(16×16)像素的图标。

e) 菜单栏的顶级标题为简明扼要的文字，除去菜单项助记符，汉字数目通常不能超过六个。

f) 如果点击菜单按钮将弹出对话框，则在菜单项助记符后以省略号“…”注明。

g) 所有出现在工具栏中的按钮都必须出现在菜单栏中。

h) 菜单层次不超过三级。

i) 各个子菜单项中的图标左对齐，没有图标的子菜单项在左侧留有空格，以使得子菜单项的文本部分左对齐。

j) 子菜单中的菜单项根据其功能上的异同进行分组，各个分组之间用一条分隔线划分。

k) 对于起开关作用的菜单项，应有开或关的状态标识，如图 5 所示；

图 5 标识控制状态

l) 对于使用频率高的菜单项设置快捷键，不必为所有的菜单项设置快捷键。

m) 如果使用弹出式菜单

1) 在重要的窗口或区域应能弹出右键，实现常用操作；

2) 弹出式菜单通过单击鼠标右键打开；

3) 右键菜单中菜单项不加图标，如有快捷键，需标明。

n) 每一个菜单项的图标必须是唯一的，不要让一个图标用于多个功能。

o) 对鼠标操作的响应

1) 当鼠标指针悬停在顶级菜单项上时，子菜单不要弹出。只有当点击后才能弹出，并且该子菜单在鼠标下次点击顶级菜单项之前一直保持弹出状态。

2) 鼠标悬停状态下，菜单选项的字体背景颜色更换为为蓝底。

右键菜单示例如图 6 所示。

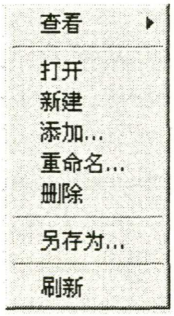

图 6 右键菜单

5.3.3 提示窗口

提示窗口要求如下：

a) 各种提示窗口应采用标准信息提示窗口以明确信息提示的类型。

b) 提示信息内容应简洁、明了、准确。提示信息结束后应该有标点，用中文全角。

c) 信息图标尺寸统一为(32×32)像素。

d) 图标应该明确显示提示、错误、警告、询问、中间出错等类型。

1) 提示窗口，该窗口用于显示需要用户知道的内容或操作执行的结果，辅助进行信息提示。窗口的按钮只包含一个【确定】按钮。提示窗口的样例如图 7 所示。

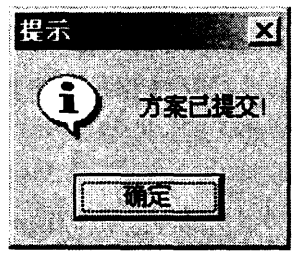

图 7 提示窗口

2) 错误信息提示窗口，该窗口应该描述错误发生原因以及如何纠正，窗口的按钮只包含一个【确定】按钮。错误信息提示窗口的样例如图 8 所示。

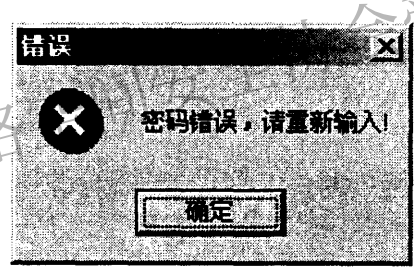

图 8 错误信息提示窗口

3) 警告窗口，该窗口用于显示接下来的操作或活动将造成的影响或危害，在该窗口中允许用户取消操作。该窗口的按钮应该包括【确定】和【取消】按钮，缺省按钮为【取消】按钮。警告窗口的样例如图 9 所示。

图 9 警告窗口

4) 询问窗口，该窗口用于询问使用者某些需要确认的内容，用于要求澄清或确认刚刚的操作目的。该窗口的按钮应该包括【是】和【否】按钮，缺省按钮为【是】按钮。询问窗口的样例如图 10 所示。

5) 中间出错窗口，该窗口用于在做较长时间的操作过程中间出现错误、异常或某些询问信息时要和使用者进行交互的情况，该窗口一般要求可以继续执行或中断该较长操作。该窗口

的按钮应该包括【终止】、【重试】和【忽略】按钮，缺省按钮应该为【重试】。

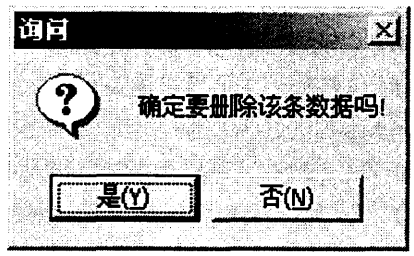

图 10　询问窗口

e) Web 风格的提示和告警主要分为两种，一是采用浏览器自身提供的功能(用 javascript 制作)，一般用于系统信息、错误的提示，如图 11 所示；二是与产品的具体功能密切的提示应采用自制的提示框，其中不仅包含传统的可操作性外，还要与产品整体的界面风格一致，如图 12 所示。按钮置于文字提示的下方。

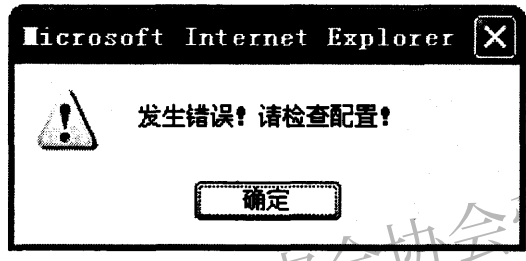

图 11　系统提示框

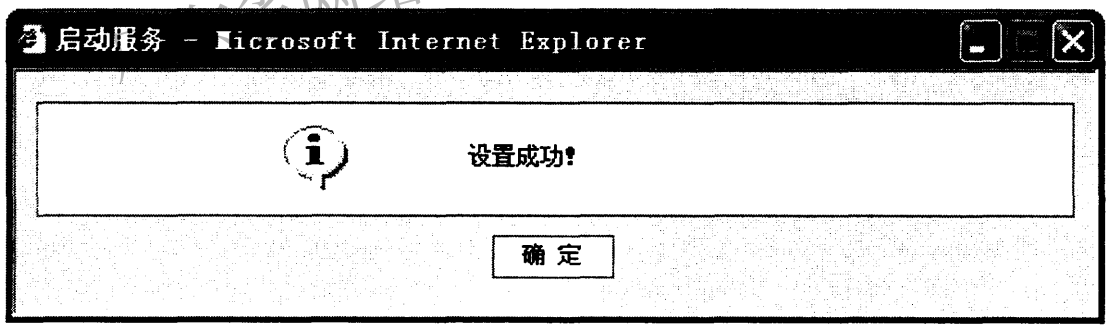

图 12　自制提示框

5.3.4　工具栏

工具栏要求如下：

a) 工具栏上放置最常用的操作按钮，必要时动态更换按钮；
b) 在窗体的工具栏中使用图标按钮，图标应能表达按钮所对应功能的意义；
c) 图标大小统一为(16×16)像素；
d) 图标采用静态图片，不增加动态效果；
e) 如果有文字，则应在图标的右方；文字为宋体九号，最多不超过四个汉字；
f) 工具栏要使用 tip(提示)方式来提示用户该按钮完成的功能，同时在状态栏显示较详细的提示说明；
g) 所有快捷按钮都可以在主菜单中找到功能对应的菜单项；
h) 当鼠标停止在快捷按钮时，按钮突出显示；
i) 工具栏中的按钮根据其功能上的异同进行分组，各个分组之间应用一条垂直分隔线进行划分。

如图 13 所示：

图 13　按钮按功能不同可被划分成几个分组

j）　一个窗口中可以包含多个工具栏，工具栏初始处于用户区上部；

k）　Web 形式管理界面上的工具栏实现结合 Web 页面的设计特点，并参考以上要求。

5.3.5　状态栏

状态栏显示正在进行的操作或当前所处的状态。

5.3.6　按钮

按钮要求如下：

a）　按钮中的文字为宋体五号字。

b）　按钮的中文字不超过三个汉字。

c）　界面中功能相近或相联系的同一组按钮的外观尺寸应该保持相同。

d）　在窗口中，有些是固定功能按钮，其名称和助记符/快捷键不应该改变，如：【确定】表示执行对窗口中控制的所有变更并关闭该窗口，不能写为【确认】、【返回】、【离开】等；【取消】表示关闭窗口而不更新该窗口中控制的所有变更，不能写为【返回】、【离开】等；但在一个界面中如果可以多次完成某项功能，如果不在主界面上，则按钮应该为【返回】按钮，表示返回上一级界面。

e）　除菜单按钮和工具栏的快捷按钮外，其他按钮一般只包含文字，不包含图标；但是如果由于界面大小限制，可以采用位图按钮，位图的大小为(16×16)像素；按钮样例如图 14 所示，左侧是一般的按钮，右侧是位图按钮。

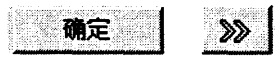

图 14　按钮

f）　对于所有的确定、取消按钮，分别用回车键、ESC 键来实现快捷键功能。

g）　如果对话框中含有确定、取消、应用和帮助按钮，则所有按钮应放在一行中，放置在对话框的右下方。

h）　使用确定、取消、应用和帮助按钮

1）　按下确定按钮后，设置生效并且关闭窗口；

2）　按下取消按钮后，关闭窗口，设置不生效；

3）　按下应用按钮后，当前设置生效，窗口不关闭；

4）　按下帮助按钮后，打开当前窗口的帮助主题；

5）　四个按钮在任何窗口中的顺序如图 15 所示。

图 15　确定、取消、应用、帮助按钮的布置顺序

5.3.7　单选按钮

单选按钮用于从成组的一套相互排斥的选项中选择一个选项。

a）　一组单选按钮要求排列整齐，间距相同；

b) 一组单选按钮应由组框框起来，以表示成组关系。如图 16 所示。

图 16 一组单选按钮

5.3.8 复选按钮

复选按钮可单独使用也可与其他检查按钮同时使用。

用于设置检查属性的复选按钮有开、关或不确定三个状态。当复选按钮的状态不确定时，用灰色填充。如图 17 所示。

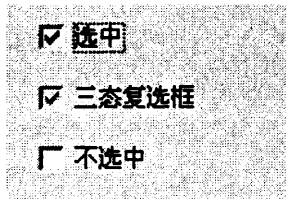

图 17 复选按钮

5.3.9 静态文本框

在窗口中静态文本框用于显示静态文字。静态文字(如：标题、题目、目录)显示在静态文本框中而不在文字编辑框中。静态文本框不可选择、编辑，其后一般跟文字编辑框、列表框、组合框等。静态文本框要求如下：

a) 静态文字编辑内容最后不得有冒号(：)；

b) 每个标签文字长度不超过 10 个全角字符。

5.3.10 文字编辑框

文字编辑框用于输入和编辑文字，要求如下：

a) 编辑框的左边或上面应有一个描述此域输入内容的静态文本框。

b) 多个编辑框之间以左侧垂直或顶端水平对齐，垂直或水平方向均匀分布，与相应的标签水平对齐。

c) 单行的文字编辑框高度要一致。

d) 如果文字编辑框输入的数字需要单位(如：米，公里)，则其右边需要加静态文本框来显示单位信息。

e) 不可编辑的编辑框使其变灰。

f) 在编辑框中进行编辑，点击回车键时不应关闭对话框。

g) 尽量在界面上限制用户不能输入非法或无效数据。如果界面上无法限制，则在用户完成编辑框的数据填写后，做必要的数据合法或有效性验证。验证时：

1) 在用户点击“确定”按钮后进行验证；

2) 经验证非法或无效后立即提示用户，说明是哪个数据填写无效，给出数据非法或无效的原因和修改建议；

3) 提示信息在当前对话框中弹出，而不要在其他窗口或对话框中显示出错信息。

5.3.11 列表框

列表框用于从一组项目中选择一个或者多个项。列表框左边或上面有一个描述选择内容的静态文本框。列表框要求如下：

a) 列表框尺寸取决于显示列表的窗口可获得空间的大小，一个列表一次足够显示六～八个项目，如果小于六个项目则显示所有项目；

b) 背景颜色为白色。

5.3.12 组合框

组合框有文字编辑框和文字编辑框下拉后立即显示的列表组成，组合框域左边或上面有一个描述选择内容的静态文本框。组合框要求如下：

a) 如果只是选择而不允许编辑，设置为下拉风格，一次足够显示六～八个项目，如果小于六个项目则显示所有项目；

b) 组合框如果允许编辑，则进行编辑后点击回车键，不应关闭对话框。

5.3.13 树型控件

树形控件要求如下：

a) 树型控件的每个节点都有图标，图标尺寸为(16×16)像素；

b) 背景颜色为白色；

c) 如果树型条目是三态的，用三种形式的图标标识，以区分全选、部分选中或不选状态；如果树型条目是两态的，用不同的图标标识选中或未选中状态。

5.3.14 表格控件

表格控件要求如下：

a) 表格的标题栏是静态的，位于表格顶层；

b) 显示表格线；

c) 标题栏的字体为宋体五号，颜色为黑色；

d) 表格中的文字为宋体五号，颜色为黑色；

e) 如果表格内容超过了显示范围，则提供相应维度上的滚动条；

f) 表格记录的相邻行用不同颜色以示区分。

5.3.15 操作进度指示

对于比较短暂的等待，应该将鼠标光标暂时变成沙漏形状，以向用户表明应该等待，并且在此过程中不能对软件进行其他操作。

对于较长时间的等待，可以使用一个工作信息提示窗口来表明工作进行的状态，并在上面显示简短的消息，描述正进行什么处理，该提示窗口在工作活动完成之前一直显示，除非用户执行取消操作(原则上漫长的操作都应该有让用户中间取消的手段)，另外应该采用进度控件来显示该过程的进展程度。如图 18 所示。

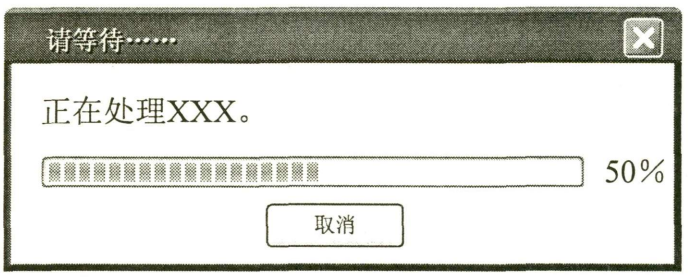

图 18 长时间等待提示窗口

5.3.16 帮助

系统应提供详尽可靠的帮助文档，使用 HTML 格式或 CHM 格式的帮助。文档要求如下：

a) 帮助文档中的功能与性能介绍与说明要与系统功能与性能配套一致，并在系统更新时做相应修改；
b) 用户可使用关键词在帮助索引中搜索所要的帮助，并应提供帮助主题词；
c) 帮助要有即时针对性，在界面上调用帮助时应该能够及时定位到与该操作相对的帮助位置；
d) 在帮助中应该提供其他技术支持方式，如电子邮件、电话、通信地址等，一旦用户难以自己解决可以方便地寻求新的帮助方式；
e) 帮助菜单中的“关于”项中应有军队版版权信息和产品信息。

5.4 操作逻辑

5.4.1 命令行

5.4.1.1 命令行要求

用户接口应可以利用 SSH 网络连接方式或串口连接方式进行命令行配置，以提供基本配置管理和灾难恢复功能，增加管理的安全、方便与灵活性。命令行要求如下：

a) 命令行界面为用户提供一个纯字符界面，向不同级别的管理员提供不同的命令集，应屏蔽管理员对文件系统的直接访问；
b) 管理员可根据实际需要决定是否启用 SSH 方式进行安全管理和维护；
c) 用户进入命令行界面后，应出现命令行提示符，用户可在命令行上输入、编辑命令；
d) 用户可以使用“？”键获得上下文相关的帮助信息，使用 TAB 键进行命令补齐；
e) 用户使用回车键提交命令；
f) 提交过的命令会储存在历史命令列表中，通过上下箭头键调用；
g) 用户可使用 CTRL＋C 中止正在执行的命令；
h) 若用户长时间(管理员可定制时间的长短)没有任何操作，命令行界面应返回到登录提示状态；
i) 客户端的连接、用户登录作息(成功或失败)、用户提交的命令、用户退出信息都应记录在系统日志中。

5.4.1.2 命令结构

命令行命令的基本结构为：“类别命令　操作类型　命令参数 1　命令参数 2　……”

a) 类别命令：表示想配置的项目，如：网络接口(if)、安全规则(rule)等；
b) 操作类型：表示对此项目进行什么样的操作，如：添加(add)、删除(del)、修改(set)、显示(show)等；
c) 命令参数：不同的操作有不同的必选或可选命令参数。

5.4.1.3 通用命令

命令行配置方式应提供的通用命令如下：

a) interface(if)；网络接口配置命令；
b) ping：网络测通；
c) arp：显示、设置网络 IP 地址与 MAC 地址之间的对应信息；
d) hostname：设置安全设备名称；
e) domain：显示、设置域名地址；
f) log：显示日志信息；
g) system 显示、设置系统信息；
h) config：系统配置命令；
i) traceroute：判定数据包到达目的主机所经过的路径；
j) help：命令帮助；
k) exit：退出命令行操作界面。

5.4.2 图形界面

图形用户界面的操作逻辑是指用户完成某个功能所需完成的操作步骤。图形界面的总体操作逻辑如图 19 所示。

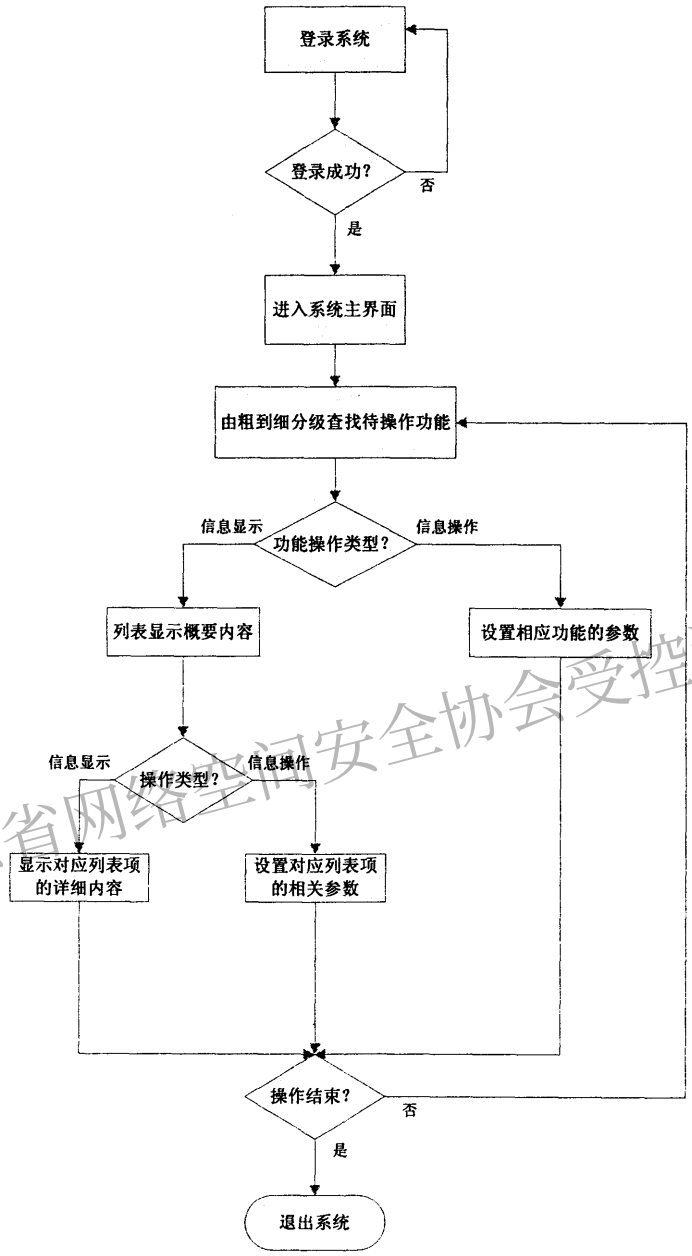

图 19　网络安全设备用户管理接口操作逻辑

用户首先登录系统，若登录成功则可以进入系统的主界面，用户在主界面中通过分级导航菜单等工具可以找到欲实现功能的菜单条目，当用户触发菜单条目后，根据操作类型不同，可以得到两种类型的界面，一种是信息显示类型的界面，以列表形式显示概要信息；另一种是信息操作类型的界面，要求用户直接在界面中录入信息或者设置参数。用户还可以对列表中的每条信息进行操作，视操作类型不同，可以显示每条信息的详细内容或者对该条信息对应的参数、状态等内容进行更改。若至此用户操作完毕，则退出系统，否则重新查找下一个欲实现功能的菜单条目。

在此流程中，用户使用管理界面的最主要操作包括三个：

a)　查找功能在主界面中的位置：用户为完成某个功能需要在主界面中查找能够触发功能实现的菜单或按钮，一般用户在菜单栏或导航菜单中进行此类查找操作；

b） 内容显示：当用户查找到功能所在位置并触发功能时，用户可以在功能显示区中查找所需的内容或设置参数；

c） 设置操作：用户可以通过设置参数和更改状态实现对系统功能的定制或者安全策略的修改。

在设计和实现上述三个功能时，应根据简洁高效的原则，尽可能简化用户操作以方便使用；同时，要协调界面色彩的明度、纯度、对比度、质感等关系，风格保持一致，使得界面色调柔和，亲和力强。

5.5 操作复杂度

用户接口操作应尽量简化，为用户提供最大程度的易用性。只抽出基本元素，让用户在使用界面时只需专注于所操作的内容，杜绝冗余、含混晦涩的复杂操作，能够合并、简化的操作尽量精简；对话框提供的内容目的明确，形式简单明了，不能只是大面积罗列控件。对于复杂的操作要用分层的方法和分粒度的方法进行简化。界面间的耦合程度要尽量减小，之间的关系要让用户一目了然。操作复杂度要求如下：

a） 操作简洁，从打开界面到完成所需操作不能超过六步；

b） 同一界面上的控件数最多不要超过 10 个，多于 10 个时可以考虑使用分页界面显示；

c） 同一操作集中完成，尽量减少用户为完成某一操作而跳转多个页面；若要使用多个页面，页面之间的逻辑关系一定要明确，操作的先后顺序一定要有提示；

d） 尽量简化用户输入，减少用户复杂的信息录入工作，多提供用户选择或自动处理功能；

e） 提供灵活的即席资源查询功能，当资源数量较多时，应分类组织内容，以方便用户查找。

5.6 用户接口安全

用户接口安全是指保护安全管理系统本身，以防止不合法的使用所造成的系统配置修改、数据泄露、数据更改或数据破坏。接口安全可分为两类：系统安全性和数据安全性。

a） 系统安全性：系统安全性是指在系统级控制安全管理系统的使用和存取的机制，包括：

1） 有效的用户名/口令的组合；

2） 某用户是否授权可操作安全管理系统；

3） 用户的资源限制；

4） 用户可执行哪些系统操作；

5） 审计信息是否有效。

b） 数据安全性是指控制操作对象的存取和使用的机制，包括：

1） 哪些用户可存取哪些指定对象及在对象上允许哪些操作类型；

2） 用户操作信息的审计内容。

网络安全设备管理接口的接口安全应实现上述两种安全机制。

5.6.1 用户权限划分

系统必须支持分级多用户服务管理，可以有多个用户同时登录系统进行操作。创建新用户时需指定用户的角色，不同角色拥有不同的操作权限。用户角色可分为：

a） 用户管理员：实现用户的增加、删除和更改等操作，同时还可以进行授权和用户封锁、解封和限时登录等功能；

b） 系统操作员：对安全系统进行操作，实现安全策略配置、资源定义等；

c） 审计管理员：确定审计内容，查看审计信息。

网络安全设备管理接口的用户权限可以是上述任意一种角色，或者是几种角色的组合。

5.6.2 授权与验证

系统中每个用户都应被限定资源的操作范围，包括：

a） 不同角色用户能够操作的对象或资源；

b） 用户允许登录的 IP 地址范围；

c） 用户允许登录系统的时间范围；

d) 用户名和口令的更改规则；

e) 用户的当前状态是被禁用或启用。

5.6.3 用户认证

用户认证是确认当前正在试图进入系统的用户就是账户数据库中记录的用户。认证用户的方法有三种：

a) 用户名/口令：对用户输入用户名和口令信息进行认证；

b) 物理识别认证：使用物理识别设备，如 IC 卡、USBKEY 等设备对用户进行识别；

c) 生物特征识别认证：使用指纹识别等技术对用户进行唯一性识别。

网络安全设备的用户接口必须提供基于用户名/口令的登录认证和身份鉴别方式。同时建议使用物理识别认证和生物识别认证方式，以支持更安全的登录认证和身份鉴别功能。安全认证系统的接口要遵循军队相关的认证系统接口规范。

5.6.4 审计

审计能够记录、确认和识别安全机制的使用、客体的使用和删除等类型的事件，还能记录操作人员和安全管理人员进行的各种活动及与安全相关的活动。

对于每个审计事件，审计记录应该包括：

a) 用户名、事件发生时间、事件类型、事件的成功与失败等；

b) 对于确认事件，请求源(如终端 ID)也应包含在审计记录中；

c) 对于客体进行访问的事件，在审计记录中还包括被访问的对象名称。

管理员可以有选择地审计某个或多个用户的活动。符合审计项的操作都记录到操作日志中，除系统审计管理员外，其他用户不能对日志进行修改和删除。

5.6.5 厂商设备代码

设备厂商子代码和厂商型号代码参见附录 C。

附 录 A
（规范性附录）
基于代理嵌入方式的系统接口

A.1 系统接口方式

A.1.1 基本要求

A.1.1.1 运行环境

接口的实现至少应能在以下操作系统中运行，并能够向其他操作系统移植：

a） Linux：内核版本 2.4.x/2.6.x；

b） Windows：Windows 98/2000/XP/2003 Server。

A.1.1.2 运行条件

一台安全设备（或服务器）上原则上只能运行一个管理代理，监听地址/端口：0.0.0.0:18000。

如果需要运行多个管理代理，则通过 A.1.3 中指定的配置信息将其他管理代理初始监听到别的端口（端口号＞18000），并通过响应 A.3.2.2 中指定的参数信息与服务器商定使用新的端口。

安全管理系统监听端口：13300。

A.1.1.3 运行资源

对磁盘空间的要求：占用不超过 10M 的磁盘空间大小（不含日志）。

对运行内存的要求：独自占用的内存空间不大于 8M。

对 CPU 占用率的要求：正常运行状态下平均不大于 2%。

A.1.2 接口说明

A.1.2.1 语法规范

本标准中的接口，基于 ISO C＋＋/STL（见 ISO/IEC 14882－2003）的语法进行描述。

A.1.2.2 命名空间

命名空间见表 A.1。

表 A.1 命名空间

命名空间	说明
SDMI::	管理代理的所有对象、方法，限定在这个命名空间中。
SDMI::Asset::	与状态视图有关的对象、方法，限定在这个命名空间中。
SDMI::Core::	与管理代理的系统框架有关的对象、方法，限定在这个命名空间中。
SDMI::Event::	与安全事件有关的对象、方法，限定在这个命名空间中。
SDMI::Policy::	与安全策略有关的对象、方法，限定在这个命名空间中。
SDMI::Util::	由实现方在标准外各自实现的工具方法，限定在这个命名空间中。

A.1.2.3 类型定义

A.1.2.3.1 类型说明

类型说明见表 A.2。

表 A.2 类型说明

名称	类型命名	说明	类型定义
代理框架类	SDMI::Core::Application	实现管理代理的基本框架。	见 A.1.2.3.2
组件类	SDMI::Core::Component	所有可加载的组件的基类，是不能实例化的抽象类。	见 A.1.2.3.3
策略执行类	SDMI::Policy::PolicyExecutor	实现对安全策略进行管理的相关功能。	见 A.1.2.3.4
状态视图类	SDMI::Asset::AssetAgent	实现对状态视图的查询和响应等相关功能。	见 A.1.2.3.5
组件管理类	SDMI::Core::Context	负责管理组件对象的注册，并将查询请求分派到已注册的对应组件上。	见 A.1.2.3.6
事件传送类	SDMI::Event::EventCP	封装上报安全事件的方法。	见 A.1.2.3.7

类型定义中提到的参数类型，见 A.2.1。各类待实现的方法见表 A.5。

各类型之间的接口调用关系如图 A.1 所示。

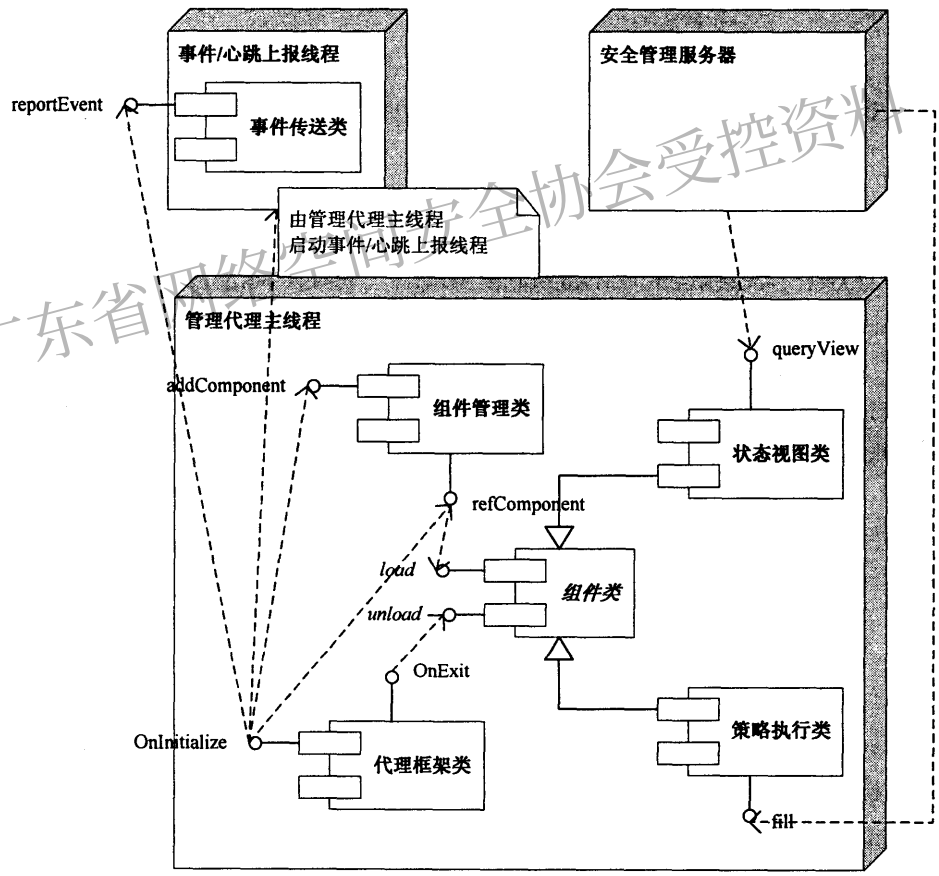

图 A.1 接口调用关系图

A.1.2.3.2 代理框架类

```
class SDMI::Core::Application
{
protected:
    virtual void OnInitialize();
    virtual void OnExit();
```

```
    public:
        SDMI::Core::Context* _context;
    };
```

A.1.2.3.3 组件类

```
    class SDMI::Core::Component
    {
    public:
        virtual bool load(SDMI::Core::Context* context, const SDMI::Core::Dict& option,
SDMI::Core::Dict& extout) = 0;
        virtual bool unload(SDMI::Core::Context* context, const SDMI::Core::Dict& option,
SDMI::Core::Dict& extout) = 0;
    };
```

A.1.2.3.4 策略执行类

```
    class SDMI::Policy::PolicyExecutor: virtual public SDMI::Core::Component
    {
    public:
        virtual bool fill(const std::string& policy, const SDMI::Core::Dict& option, SDMI::Core::Dict&
extout);
    };
```

A.1.2.3.5 状态视图类

```
    class SDMI::Asset::AssetAgent: virtual public SDMI::Core::Component
    {
    public:
        virtual std::string queryView(const std::string& viewTypeId, const SDMI::Core::Dict& option,
SDMI::Core::Dict& extout);
    };
```

A.1.2.3.6 组件管理类

```
    class SDMI::Core::Context
    {
    public:
        virtual bool addComponent(const std::string& comid, SDMI::Core::Component* component,
const SDMI::Core::Dict& option, SDMI::Core::Dict& extout);
        virtual bool refComponent(const std::string& type, const std::string& comid, const
SDMI::Core::Dict& option, SDMI::Core::Dict& extout);
    }
```

A.1.2.3.7 事件传送类

```
    class SDMI::Event::EventCP
    {
    public:
        bool reportEvent(const SDMI::Core::Dict& event, const SDMI::Core::Dict& option,
SDMI::Core::Dict& extout);
    }
```

A.1.2.4 工作时序

A.1.2.4.1 内部工作时序

安全设备和管理代理，以及管理代理内部的工作时序如图 A.2 所示。

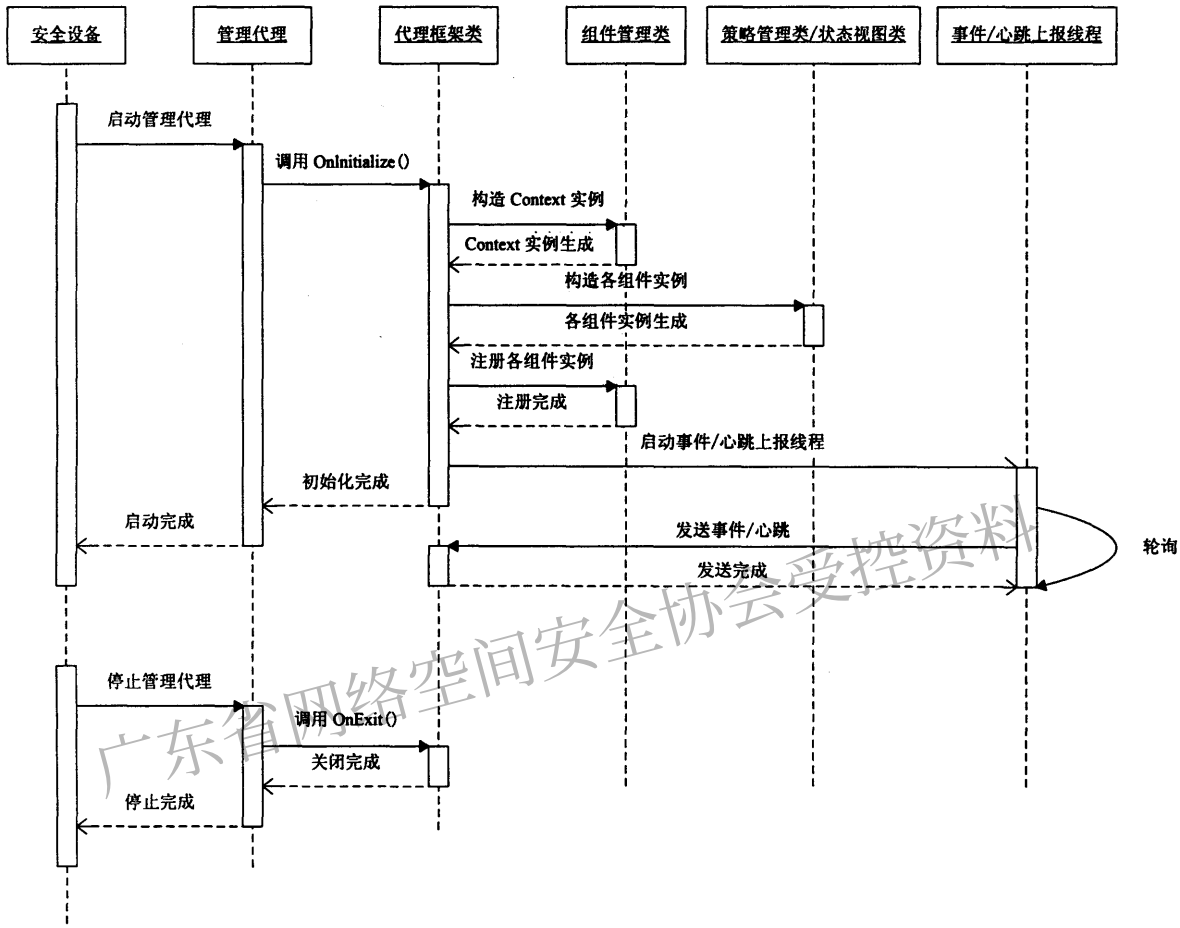

图 A.2 接口内部工作时序图

A.1.2.4.2 外部工作时序

安全管理系统和管理代理、安全设备之间的工作时序如图 A.3 所示。

A.1.2.5 接口功能

A.1.2.5.1 安全管理系统

在本接口中，安全管理系统需要实现的功能见表 A.3。

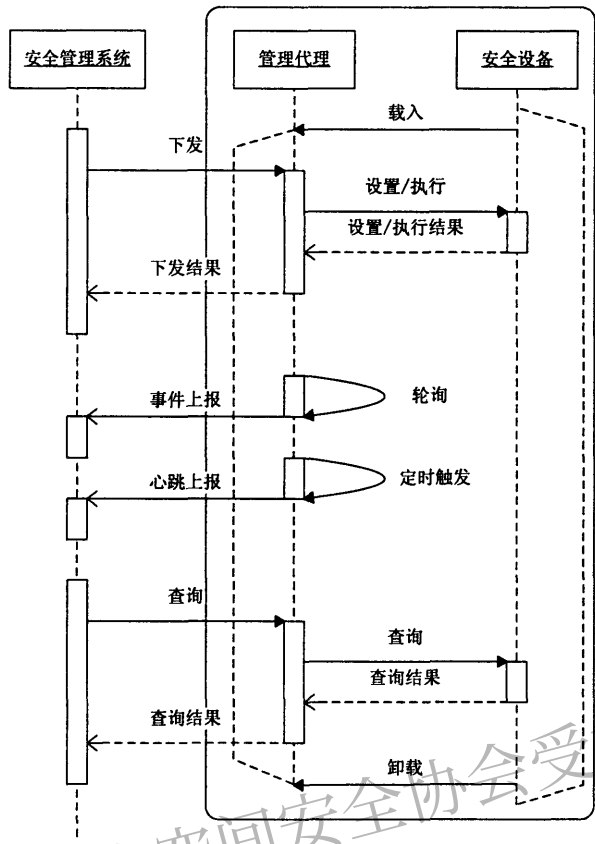

图 A.3　接口外部工作时序图

表 A.3　安全管理系统接口功能表

接口功能	实现内容	说明	接口方法
设备参数配置	设备参数下发	通过接口下发参数配置信息给设备	SDMI::Policy::PolicyExecutor::fill 见 A.1.2.6
	设备参数查询	通过接口从设备查询设备参数配置	SDMI::Asset::AssetAgent::queryView 见 A.1.2.6
安全策略管理	安全策略下发	通过接口下发安全策略给设备	SDMI::Policy::PolicyExecutor::fill 见 A.1.2.6
	安全策略查看	通过接口从设备查询当前运行的安全策略	SDMI::Asset::AssetAgent::queryView 见 A.1.2.6
事件管理	事件接收	通过接口接收从设备上报的安全事件	SDMI::Event::EventCP::reportEvent 见 A.1.2.6
设备状态与性能监视	设备状态查询	通过接口从设备查询当前状态信息	SDMI::Asset::AssetAgent::queryView 见 A.1.2.6
维护性操作	操作下发	通过接口下发操作给设备	SDMI::Policy::PolicyExecutor::fill 见 A.1.2.6
系统接口安全	双向鉴别认证	通过接口与安全设备交换证书	见 A.1.4.1
	通讯保护	用证书对通讯进行保护	见 A.1.4.2

A.1.2.5.2 安全设备

在本接口中，安全设备需要实现的功能见表 A.4。

表 A.4 安全设备接口功能表

接口功能	实现内容	说明	接口方法
设备参数配置	设备参数接收	接收安全管理系统下发的参数配置信息	SDMI::Policy::PolicyExecutor::fill 见 A.1.2.6
	设备参数设置	配置设备使用收到的参数配置	SDMI::Policy::PolicyExecutor::fill 见 A.1.2.6
	响应设备参数查询	响应安全管理系统通过接口发起的查询请求	SDMI::Asset::AssetAgent::queryView 见 A.1.2.6
安全策略管理	安全策略接收	接收安全管理系统下发的安全策略	SDMI::Policy::PolicyExecutor::fill 见 A.1.2.6
	安全策略执行	配置设备执行收到的安全策略	SDMI::Policy::PolicyExecutor::fill 见 A.1.2.6
	响应安全策略查看	响应安全管理系统通过接口发起的查询请求	SDMI::Asset::AssetAgent::queryView 见 A.1.2.6
事件管理	事件的采集和上报	通过接口向安全管理系统上报安全事件	SDMI::Event::EventCP::reportEvent 见 A.1.2.6
设备状态与性能监视	响应设备状态查询	响应安全管理系统通过接口发起的查询请求	SDMI::Asset::AssetAgent::queryView 见 A.1.2.6
维护性操作	操作接收	接收安全管理系统下发的操作	SDMI::Policy::PolicyExecutor::fill 见 A.1.2.6
	操作执行	配置设备执行收到的操作	SDMI::Policy::PolicyExecutor::fill 见 A.1.2.6
系统接口安全	双向鉴别认证	通过接口与安全管理系统交换证书	见 A.1.4.1
	通讯保护	用证书对通讯进行保护	见 A.1.4.2
	操作审计	通过接口向安全管理系统上报管理日志	见 A.1.4.3

A.1.2.6 方法说明

接口方法说明见表 A.5。

表 A.5　接口方法列表

序号	命名空间	方法	功能用途	实现位置	参数说明		返回值说明
					参数名	说明	
1	SDMI::Core::	void Application::OnInitialize();	管理代理启动时自动调用此方法。 实现方在此方法中实现管理代理的初始化逻辑。	安全设备	无	无	无
2		void Application::OnExit();	管理代理停止时自动调用此方法。 实现方在此方法中实现管理代理的关闭逻辑。	安全设备	无	无	无
3		void Context::addComponent(const std::string& comid, Component* component, const SDMI::Core::Dict& option, SDMI::Core::Dict& extout);	安全设备在管理代理的代理框架中调用此方法把指定的组件注册到一个内部数据结构中。 实现方在此方法中实现该内部数据结构，并进行组件注册。	安全管理系统	comid	组件 ID，在同一个管理代理中需要唯一。唯一性由调用方确保。	无
					component	需要注册的组件，必须是组件类的派生类，即策略执行类或状态视图类的指针。	
					option	调用选项，目前不使用。	
					extout	扩展输出。用于返回执行的结果，如执行正常，则无需输出。取值见表 A.6。	
4		void Context::refComponent(const std::string& type, const std::string& comid, const SDMI::Core::Dict& option, SDMI::Core::Dict& extout);	安全设备在管理代理的代理框架中调用此方法把设备参数配置、安全策略、状态视图或维护性操作绑定到指定的组件上。 实现方在此方法中确定设备参数配置、安全策略、状态视图或维护性操作和组件的绑定关系并保存。	安全管理系统	type	欲绑定到组件上的设备参数配置、安全策略、状态视图或维护性操作的类型代码。见 A.2.3.2、A.2.3.3、A.2.3.4 、 A.2.3.5 、A.3.5。	无

表 A.5(续)

序号	命名空间	方法	功能用途	实现位置	参数说明		返回值说明
					参数名	说明	
4	SDMI::Core::	void Context::refComponent(const std::string& type, const std::string& comid, const SDMI::Core::Dict& option, SDMI::Core::Dict& extout);	安全设备在管理代理的代理框架中调用此方法把设备参数配置、安全策略、状态视图或维护性操作绑定到指定的组件上。 实现方在此方法中确定设备参数配置、安全策略、状态视图或维护性操作和组件的绑定关系并保存。	安全管理系统	comid	欲绑定组件的组件ID。见 addComponent 方法。	
					option	调用选项，目前不使用。	
					extout	扩展输出。用于返回执行的结果，如执行正常，则无需输出。取值见表 A.6。	
5	SDMI::Event::	bool EventCP::reportEvent(const SDMI::Core::Dict& event, const SDMI::Core::Dict& option, SDMI::Core::Dict& extout);	安全设备调用此方法向安全管理系统发送安全事件。 实现方在此方法中完成发送安全事件的功能。	安全管理系统	event	包含 IDMEF 消息的 Dict 对象。其键值取 IDMEF 消息格式中的字段名。见 A.4。	true：成功 false：失败
					option	调用选项，目前不使用。	
					extout	扩展输出，目前不使用。	
6	SDMI::Policy::	bool PolicyExecutor::load(SDMI::Core::Context* context, const SDMI::Core::Dict& option, SDMI::Core::Dict& extout);	当策略执行类对象在组件管理类中进行注册后，此方法被调用。 实现方在此方法中完成对策略执行类必要的初始化工作。	安全设备	context	组件管理类的实例。	true：成功。如有警告，用 extout 输出。 false：失败。需要说明原因，用 extout 输出。
					option	调用选项，目前不使用。	
					extout	扩展输出。用于返回执行的结果，如执行正常，则无需输出。取值见表 A.6。	

表 A.5(续)

序号	命名空间	方法	功能用途	实现位置	参数说明		返回值说明
					参数名	说明	
7	SDMI::Policy::	bool PolicyExecutor::fill(const std::string& policy, const SDMI::Core::Dict& option, SDMI::Core::Dict& extout);	安全管理系统调用本方法向安全设备推送设备参数、安全策略或维护性操作。 实现方在此方法中对设备参数、安全策略或操作进行解析、执行，并返回结果。	安全设备	policy	安全策略。以 XML 形式的设备参数、安全策略或维护性操作，采用 utf-8 编码格式。见 A.3.2、A.3.3、A.3.5。	true：成功。如有警告，用 extout 输出。 false：失败。需要说明原因，用 extout 输出。
					option	调用选项，目前不使用。	
					extout	扩展输出。用于返回执行的结果，如执行正常，则无需输出。取值见表 A.6。	
8		bool PolicyExecutor::unload(SDMI::Core::Context* context, const SDMI::Core::Dict& option, SDMI::Core::Dict& extout);	管理代理调用此方法卸载策略执行类的对象。 实现方在此方法中实现对策略执行类必要的结束工作。	安全设备	context	组件管理类的实例。	true：成功。如有警告，用 extout 输出。 false：失败。需要说明原因，用 extout 输出。
					option	调用选项，目前不使用。	
					extout	扩展输出。用于返回执行的结果，如执行正常，则无需输出。取值见表 A.6。	
9	SDMI::Asset::	bool AssetAgent::load(SDMI::Core::Context* context, const SDMI::Core::Dict& option, SDMI::Core::Dict& extout);	当状态视图类对象在组件管理类中进行注册后，此方法被调用。 实现方在此方法中完成对状态视图类必要的初始化工作。	安全设备	context	组件管理类的实例。	true：成功。如有警告，用 extout 输出。 false：失败。需要说明原因，用 extout 输出。
					option	调用选项，目前不使用。	
					extout	扩展输出。用于返回执行的结果，如执行正常，则无需输出。取值见表 A.6。	

表 A.5(续)

序号	命名空间	方法	功能用途	实现位置	参数说明		返回值说明
					参数名	说明	
10	SDMI::Asset::	string AssetAgent::queryView(const std::string& viewTypeId, const SDMI::Core::Dict& option, SDMI::Core::Dict& extout);	安全管理系统调用本方法向安全设备查询状态视图。 实现方在此方法中生成状态视图，并返回结果。	安全设备	viewTypeID	状态视图类型代码。见 A.2.3.4。	string，XML格式的状态视图数据，采用 utf-8 编码。 见 A.3.3.8。
					option	调用选项，取值见表 A.7。	
					extout	扩展输出。用于返回执行的结果，如执行正常，则无需输出。取值见表 A.6。	
11		bool AssetAgent::unload(SDMI::Core::Context* context, const SDMI::Core::Dict& option, SDMI::Core::Dict& extout);	管理代理调用此方法卸载状态视图类的对象。 实现方在此方法中实现对状态视图类必要的结束工作。	安全设备	context	组件管理类的实例。	true：成功。如有警告，用 extout 输出。 false：失败。需要说明原因，用 extout 输出。
					option	调用选项，目前不使用。	
					extout	扩展输出。用于返回执行的结果，如执行正常，则无需输出。取值见表 A.6。	

表 A.6　方法调用扩展输出表

键	取值	说明
code	字符串，见 A.2.3.8	差错代码，没有此内容则填写空字符串
error	字符串，编码方式见 GB 2312－1980	错误信息，没有此内容则填写空字符串
warning	字符串，编码方式见 GB 2312－1980	警告信息，没有此内容则填写空字符串

表 A.7　状态视图查询扩展参数表

键	取值	说明
targetip	字符串	欲转发安全策略的目标 IP，逗号分隔，不需要转发则填空字符串
keyid	字符串	欲查询内容的键值
keyid2	字符串	(如果需要两个键值才传入此值)欲查询内容的键值 2
……		依次规律进行迭代至 n
keyidn	字符串	(如果需要两个键值才传入此值)欲查询内容的键值 2
其他		保留给安全管理系统和安全设备厂家用于扩展接口功能

A.1.3　代理配置

管理代理配置参数见表 A.8。

表 A.8　代理配置参数表

参数	说明
SDMI.Adapter.Endpoints	代理的侦听地址、端口、协议
ConnectTimeout	网络 TCP 连接超时，单位毫秒
Timeout	网络数据传送超时，单位毫秒
MessageSizeMax	网络协议允许传输的最大消息尺寸，单位：字节

A.1.4　接口安全

A.1.4.1　双向鉴别认证

被管安全设备与安全管理系统之间支持基于数字证书的双向鉴别认证机制，管理员在登记设备时上传安全管理系统的信任根证书到设备内，建立信任关系。此后基于该数字证书完成接口调用过程中的设备到安全管理系统、安全管理系统到设备的双向认证，如果认证失败则通讯双方无法建立接口调用所需的网络连接。证书采用 X.409 格式(见 IETF RFC2459)。

A.1.4.2　通讯保护

被管安全设备与安全管理系统之间的接口调用所基于的网络通讯采用 SSL/TLS(见 IETF RFC2246)进行保护，防止内容被非法篡改、防止数据包的重放攻击、防止网络中间人攻击。

A.1.4.3　操作审计

所有通过本接口对安全设备的管理操作，在安全设备上形成管理日志。

管理日志的大小控制在 10M 之内，循环使用日志存储空间，其容量下限由安全设备的存储能力决定。

管理日志中至少应包括内容见表 A.9。

表 A.9 审计日志表

参数名	说明
时间	操作发生的时间，IDMEF 时间戳格式，见 A.2.1.2.2
安全管理系统 IP	IP 地址
操作内容	自定义字符串
操作对象	自定义字符串
操作结果	自定义字符串

安全设备通过安全事件上报接口把日志上传到安全管理系统，见 A.1.2.6。

A.1.5 差错控制

管理代理的接口函数提供了统一的结果与差错返回方式，其基本流程如图 A.5 所示。

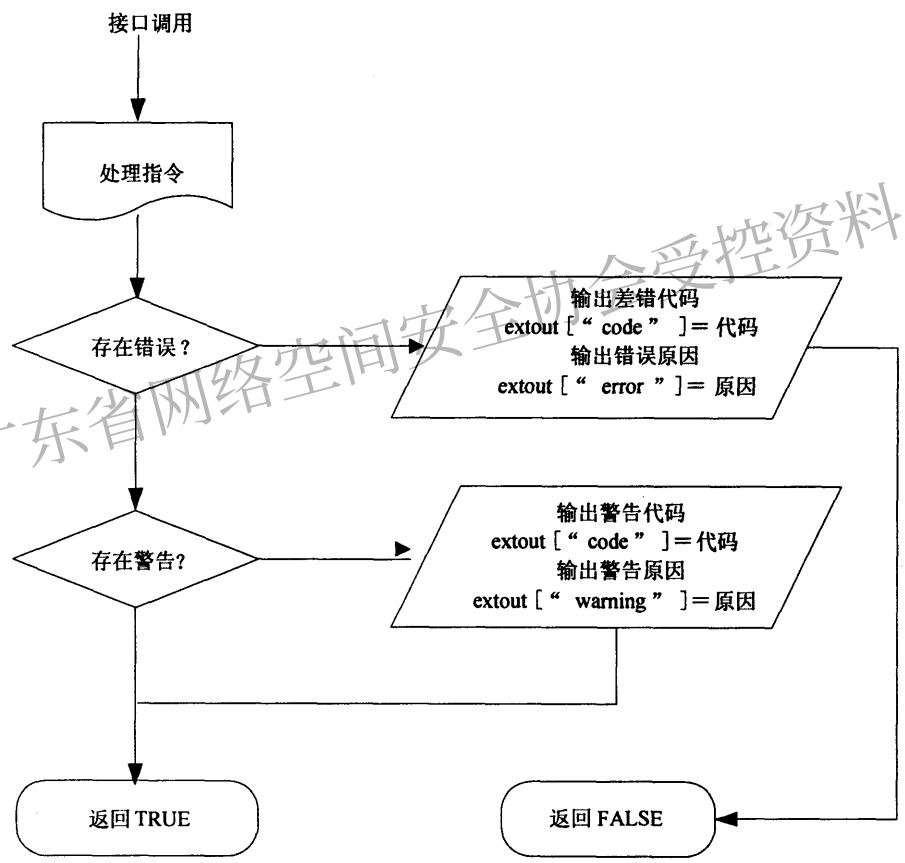

图 A.5 差错控制流程图

输出有两个地方：Dict 型参数 extout 和返回值，如果在指令执行过程中发生警告或者错误，则需通过 extout 输出差错代码和信息，返回值只有对于错误情况才返回 false。

PolicyExecutor 和 AssetAgent 这两个接口对象中的接口函数需要按照上述方式返回差错信息。错误代码见 A.2.3.8。

A.2 公用信息

A.2.1 数据类型

A.2.1.1 接口参数类型

安全管理系统与安全设备之间的接口需要用到的基本数据类型，见表 A.10。

表 A.10 接口参数类型表

数据类型	说明	取值范围	备注
string	字符串类型	0～2147483648 字节	C++STL 定义的类型
bool	布尔类型	true/false	C++类型
int	整型	0～2147483648	C++类型
Dict	map<string，string>类型	无	基于 C++ STL 模板类定义而成
SDMI::Core::Component *	指向组件类的指针	无	组件类的定义见 A.1.2.3.3
SDMI::Core::Context*	指向组件管理类的指针	无	组件管理类的定义见 A.1.2.3.6

A.2.1.2 时间戳类型

A.2.1.2.1 NTP 时间戳格式

NTP 用时间戳表示为一 64 bits unsigned 定点数，以秒的形式从 1900 年 1 月 1 日的 0：0：0 算起。整数部分在前 32 位里，后 32bits(Seconds Fraction)用以表示秒以下的部分。在 Seconds Fraction 部分，无意义的低位应该设置为 0。见 IETF RFC1769。

A.2.1.2.2 IDMEF 时间戳格式

在 IDMEF 中 NTP 时间戳格式必须被表示成两个 16 进制的 32 位整数。见 IETF RFC4765。

A.2.2 公用 XML 片段

A.2.2.1 创建/更新时间

用于标识信息的创建或更新时间。DTD 如下：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- CreateTime.dtd -->
<!ELEMENT CreateTime (#PCDATA)>
<!ATTLIST CreateTime
    ntpstamp CDATA #REQUIRED
>
```

其中，ntpstamp 属性为 NTP 格式时间戳，标签内文本为 IDMEF 格式时间戳，两者表达的值必须一致。两种时间戳见 A.2.1.2。

A.2.2.2 可选参数

用于在保留协议扩展性前提下方便地表示各种参数。DTD 如下：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- AdditionalData.dtd -->
<!ENTITY % attvals.adtype "
    ( boolean | byte | character | date-time | integer | ntpstamp |
     portlist | real | string | byte-string | xml )
">
<!ELEMENT AdditionalData ((boolean | byte | character | date-time | integer | ntpstamp | portlist | real | string | byte-string | xml))>
<!ATTLIST AdditionalData
    type %attvals.adtype; "string"
    meaning CDATA #IMPLIED
>
<!ELEMENT boolean (#PCDATA)>
```

```
<!ELEMENT byte (#PCDATA)>
<!ELEMENT character (#PCDATA)>
<!ELEMENT date－time (#PCDATA)>
<!ELEMENT integer (#PCDATA)>
<!ELEMENT ntpstamp (#PCDATA)>
<!ELEMENT portlist (#PCDATA)>
<!ELEMENT real (#PCDATA)>
<!ELEMENT string (#PCDATA)>
<!ELEMENT byte－string (#PCDATA)>
```

其中，meaning 属性为可选参数的名称或注释等说明性文字。type 和 Additional 内部包含的标签名表示了可选参数的类型，两者的表达必须一致。Additional 内部包含的标签内的文本为可选参数的值。

A.2.2.3 地址标签

用于表示各种地址信息。DTD 如下：

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ Address.dtd －－>
<!ENTITY % attvals.addrcat "
    ( unknown | atm | e－mail | lotus－notes | mac | sna | vm |
   domain－name| xstf－path | ipv4－addr－range | ipv6－addr－range |
    ipv4－addr | ipv4－addr－hex | ipv4－net | ipv4－net－mask |
    ipv6－addr | ipv6－addr－hex | ipv6－net | ipv6－net－mask )
">
<!ELEMENT Address (address, netmask?)>
<!ATTLIST Address
   ident CDATA "0"
   category %attvals.addrcat; "unknown"
   vlan－name CDATA #IMPLIED
   vlan－num CDATA #IMPLIED
   name CDATA #IMPLIED
>
<!ELEMENT address (#PCDATA)>
<!ATTLIST address
   addrassign (static | pppoe | ppp | dhcp) #IMPLIED
>
<!ELEMENT netmask (#PCDATA)>
```

A.2.3 公用代码

A.2.3.1 设备类型代码

标识安全设备类型的代码类型为字符串。

目前已有的代码见表 A.11，新增设备类型采用类型英文名称字符串作为设备类型代码。

表 A.11 设备类型代码

代码	说明
Firewall	防火墙设备
IDS	入侵检测设备

表 A.11(续)

代码	说明
AntiVirus	防病毒
Isolation	网络隔离设备
Vulnerability	漏洞扫描设备
PME	授权管理
DatabaseAudit	数据库审计
PatchMgr	补丁分发管理
EndpointSecurity	主机监控

A.2.3.2 设备参数配置类型代码

设备参数配置类型的代码类型为字符串。

设备参数配置类型代码由“设备参数配置名称_设备参数配置版本”组成，其中“设备参数配置名称”和“设备参数配置版本”为变量，下划线为字符串常量。目前已有的代码见表 A.12。

表 A.12 设备参数配置类型代码

代码	说明
SDMI_1.00	系统接口参数
Interfaces_1.00	设备网络接口参数
RouteTable_1.00	网络路由表参数

A.2.3.3 安全策略类型代码

安全策略类型的代码类型为字符串。

安全策略类型代码由“安全策略名称_安全策略版本”组成，其中“安全策略名称”和“安全策略版本”为变量，下划线为字符串常量。目前已有的代码见表 A.13。

表 A.13 安全策略类型代码

代码	说明
IpAcl_1.00	IP 访问控制策略
NAT_1.00	地址转换策略
IDS_1.00	入侵检测策略
VirusDetect_1.00	实时病毒检测策略
ActiveDefense_1.00	主动防御策略
VirusScanTask _1.00	定时病毒扫描任务策略
VirusScan_1.00	手动/快捷病毒扫描策略
AUDIT_SERVER_CONF_MGM_1.00	数据库审计策略
Vulnerability_1.00	漏洞扫描策略
PATCH-DOWN-CONTROL_1.00	人工选择补丁分发策略
PATCH-CLIENT-CONTROL_1.00	补丁自动分发策略
DevCtrl_2.00	外设控制策略
HostUA_2.00	用户认证策略
OCMonitor_2.00	外联监控策略
ContainerGuard_2.00	代理保护策略

A.2.3.4 状态视图类型代码

状态视图类型的代码类型为字符串。

状态视图类型代码由“状态视图名称_状态视图版本”组成，其中“状态视图名称”和“状态视图版本”为变量，下划线为字符串常量。目前已有的代码见表 A.14。

表 A.14 状态视图类型代码

代码	说明
sys-info_1.00	设备系统信息视图
net-info_1.00	网络状态信息视图
conn-track_1.00	连接状态信息视图
health-index_1.00	系统健康指数视图
agent-info_1.00	代理接口信息视图
idsengin-info_1.00	入侵检测引擎信息视图
avengin-info_1.00	病毒检测引擎信息视图
IpAcl-View_1.00	IP 访问控制规则视图
NAT_1.00	地址转换策略回显视图
IDS_1.00	入侵检测策略回显视图
VirusDetect_1.00	实时病毒扫描策略回显视图
ActiveDefense_1.00	主动防御策略回显视图
VirusScanTask _1.00	病毒扫描任务策略回显视图
VirusScan_1.00	手动和快捷病毒扫描策略回显视图
reg-info_view_1.00	注册信息视图
Isolation-policy_view_1.00	隔离策略视图
AUDIT_SERVER_AUDIT_VIEW_1.00	审计节点审计管理视图
AUDIT_SERVER_CONF_VIEW_1.00	审计节点配置管理视图
ORACLE_INFO_VIEW_1.00	Oracle 信息视图
SEC_SERVER_CONF_VIEW_1.00	访问控制节点配置管理视图
SEC_SERVER_SEC_VIEW_1.00	访问控制节点安全管理视图
SYS_VIEW_1.00	系统管理视图
Vulengin-info_1.00	漏洞扫描引擎视图
VulnerabilityPolicy_1.00	漏洞扫描策略视图
VulnerabilityList_1.00	漏洞扫描任务列表视图
VulnerabilityResult_1.00	漏洞扫描结果视图
VulInfo_1.00	漏洞信息视图
PATCH-CLIENT-CONTROL-VIEW_1.00	人工选择补丁分发策略视图
PATCH-DOWN-CONTROL-VIEW_1.00	补丁自动分发策略视图
Patch-Info_1.00	补丁安装信息视图
Patch-List_1.00	补丁库列表视图
DevCtrl_2.00	外设控制策略回显视图

表 A.14(续)

代码	说明
HostUA_2.00	用户认证策略回显视图
OCMonitor_2.00	外联监控策略回显视图
IpAcl_1.00	IP 防火墙策略回显视图
ContainerGuard_2.00	代理保护策略回显视图
hw-hostgroup-list_1.00	主机组列表信息视图
host-list_1.00	主机列表信息视图
hw-usergroup-list_1.00	用户组列表信息视图
hw-user-list_1.00	用户列表信息视图
hw-server_stat_1.00	服务器统计信息视图

A.2.3.5 操作类型代码

操作类型的代码类型为字符串。

操作类型代码由“操作名称_操作版本”组成，其中“操作名称”和“操作版本”为变量，下划线为字符串常量。目前已有的代码见表 A.15。

表 A.15 操作类型代码

代码	说明
Operation_1.00	通用维护性操作
VirusScan_1.00	病毒扫描操作
VulScan_1.00	漏洞扫描操作

A.2.3.6 安全事件源厂商型号代码

A.2.3.6.1 编码规则

安全事件源厂商型号的代码是由 8 位十进制数字组成的字符串，见图 A.6：

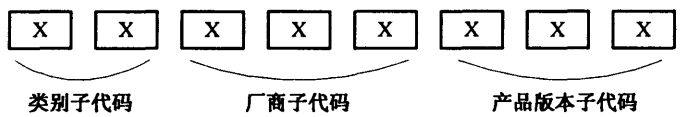

图 A.6 安全事件源厂商型号代码编码图

从左至右，第 1～2 位标识设备类别，第 3～5 位标识厂商，第 5～8 位标识设备版本。

A.2.3.6.2 设备类别子代码

设备类别子代码见表 A.16，新增加设备类型时按数字递增进行编码。

表 A.16 设备类别子代码

设备类型	类别编码
防火墙设备	06
入侵检测设备	05
防病毒	07
网络隔离设备	06
漏洞扫描设备	04

表 A.16(续)

设备类型	类别编码
授权管理	03
数据库审计	02
补丁分发管理	08
主机监控设备	08
网络安全管理设备	09

A.2.3.6.3 设备厂商子代码

设备厂商子代码参见附录C，新增加设备厂商时按数字递增进行编码。

A.2.3.6.4 厂商型号代码

目前已有的厂商型号代码参见附录C，新增加厂商型号时按数字递增进行编码。

A.2.3.7 安全事件源类别代码

安全事件源类别的代码类型为字符串。

在设备类型代码表中已有的类型，安全事件源类型代码使用对应的设备类型代码。否则使用设备类型的英文单词作安全事件源类型的代码加入代码表中。目前已有的代码见表A.17。

表 A.17 安全事件源类别代码

代码	说明
SOC	安全管理、运维系统
HeartBeat	心跳事件
外设控制	主机外设访问控制模块
IP 防火墙	主机 IP 防火墙模块
安全属性	主机代理安全保护模块
用户认证	主机用户登录认证
外联监控	主机外联监控模块
主机信息	主机信息采集模块
接入发现	主机接入发现模块

A.2.3.8 错误代码

错误代码为字符串。错误代码见表A.18。

设备在响应服务器的指令时，如果有差错，必须正确返回给安全管理服务。差错的类型有两种：

a) 错误：对指令的执行产生致命影响的结果；

b) 警告：不影响指令的正常执行，只是在执行过程中有一定的偏差。

表 A.18 错误代码

代码	类型	名称	备注
E1000	错误	设备内部错误	设备执行过程中发生内部错误
E1001	错误	安全策略格式错误	安全策略 XML 与规范不一致，存在语法错误
E1002	错误	安全策略配置项不正确	安全策略中配置的参数有问题或者存在冲突，需要更改配置项
E1003	错误	安全策略配置项不完整	安全策略中配置不全导致安全策略无法正常执行，需要补充配置项

表 A.18(续)

代码	类型	名称	备注
E1004	错误	安全策略所依赖的其他安全策略未配置	所依赖的安全策略必须先被分发执行
E1005	错误	无法访问目标设备	目标设备网络不可达，或者管理代理故障
E1006	错误	设备不支持所分发的安全策略	所分发的安全策略类型在设备端不支持
E1007	错误	安全策略分发执行超时	设备未及时反馈执行结果
E1008	错误	设备认证失败	设备对服务器的单向认证未通过
E1009	错误	状态数据格式错误	设备返回的状态数据格式不符合规范，存在语法错误
E1010	错误	设备无法获取状态数据	设备因故障无法正确获取设备状态数据
E1011	错误	获取状态数据超时	设备响应查询请求的时间超时
E1012	错误	设备不支持所查询的状态	所查询的状态数据的类型在设备端不支持
E1013	错误	操作请求格式错误	操作请求 XML 数据格式不符合规范，存在语法错误
E1014	错误	操作配置项不正确	操作中配置的参数有问题或者存在冲突，需要更改配置项
E1015	错误	操作配置项不完整	操作中配置不全导致操作无法正常执行，需要补充配置项
E1016	错误	设备操作超时	设备响应操作请求的时间超时
E1017	错误	设备不支持所请求的操作	所请求的操作类型在设备端不支持
E1018	错误	设备正忙无法响应请求	上次同样请求的操作还未完成
W1001	警告	安全策略中某些配置项不支持	安全策略中的某些配置在设备端不再被支持，但其他配置项都被正常执行
W1002	警告	安全策略未变更	安全策略没有被修改过，当前分发的安全策略在设备端已经被执行了

A.2.4 设备标识

A.2.4.1 本级设备的标识

设备标识用于对安全设备进行唯一标识，格式为“/设备名称”，其中字符“/”表示本级，“设备名称”部分由数字、字母和中文字符构成，不能包含“空格 下划线 \:"*?<>| ”。例如：“/内网防火墙”、“/FirewallA”、“/Firewall-192.168.0.3”等。

不同类型的设备，如防火墙、入侵检测设备等的标识必须唯一，其命名空间为本级，即，在本级内唯一。

A.2.4.2 下级设备的标识

格式为“/域名称/设备名称”，其中字符“/”表示级，“域名称”由数字、字母和中文字符构成，不能包含“空格 下划线\:"*?<>|”。“设备名称”同本级设备的格式一致。用多个“/”串联表示多个域的级联。例如：“/空军/指挥所 1/防火墙 A”。

A.3 参数封包说明

A.3.1 实现说明

A.3.1.1 最低实现

各设备至少要支持的参数封包如表 A.19。不在此表中的参数封包，由各厂商视各自安全设备的能力而定。

表 A.19 必须实现的参数封包列表

设备类型	参数封包类型	参数封包类型代码	说明	参数封包内容
防火墙设备	设备参数	SDMI_1.00	系统接口参数	见 A.3.2.2
		Interfaces_1.00	设备网络接口参数	见 A.3.2.3
		RouteTable_1.00	网络路由表参数	见 A.3.2.4
	安全策略	IpAcl_1.00	IP 访问控制策略	见 A.3.3.2.1
		NAT_1.00	地址转换策略	见 A.3.3.2.2
	状态视图	sys-info_1.00	设备系统信息视图	见 A.3.4.3.2.1
		net-info_1.00	网络状态信息视图，包括：网口信息、路由信息	见 A.3.4.3.2.2
		conn-track_1.00	连接状态信息视图	见 A.3.4.3.2.3
		health-index_1.00	系统健康指数视图	见 A.3.4.3.2.4
		agent-info_1.00	代理接口信息视图	见 A.3.4.3.2.5
		IpAcl-View_1.00	IP 访问控制规则视图	见 A.3.4.3.3
		NAT_1.00	地址转换策略回显视图	见 A.3.4.1
	维护性操作	Operation_1.00	通用维护性操作	见 A.3.5.1
入侵检测设备	设备参数	SDMI_1.00	系统接口参数参数	见 A.3.2.2
		Interfaces_1.00	设备网络接口参数	见 A.3.2.3
		RouteTable_1.00	网络路由表参数	见 A.3.2.4
	安全策略	IDS_1.00	入侵检测策略	见 A.3.3.3
	状态视图	sys-info_1.00	设备系统信息视图	见 A.3.4.3.2.1
		net-info_1.00	网络状态信息视图，包括：网口信息、路由信息	见 A.3.4.3.2.2
		conn-track_1.00	连接状态信息视图	见 A.3.4.3.2.3
		health-index_1.00	系统健康指数视图	见 A.3.4.3.2.4
		agent-info_1.00	代理接口信息视图	见 A.3.4.3.2.5
		idsengin-info_1.00	入侵检测引擎信息视图	见 A.3.4.3.4
		IDS_1.00	入侵检测策略回显视图	见 A.3.4.1
	维护性操作	Operation_1.00	通用维护性操作	见 A.3.5.1
防病毒	设备参数	SDMI_1.00	系统接口参数	见 A.3.2.2
	安全策略	VirusDetect_1.00	实时病毒检测策略	见 A.3.3.4.1
		ActiveDefense_1.00	主动防御策略	见 A.3.3.4.2
		VirusScanTask _1.00	定时病毒扫描任务策略	见 A.3.3.4.3
		VirusScan_1.00	手动/快捷病毒扫描策略	见 A.3.3.4.4
	状态视图	sys-info_1.00	设备系统信息视图	见 A.3.4.3.2.1
		health-index_1.00	系统健康指数视图	见 A.3.4.3.2.4
		agent-info_1.00	代理接口信息视图	见 A.3.4.3.2.5
		avengin-info_1.00	病毒检测引擎信息视图	见 A.3.4.3.5

表 A.19(续)

设备类型	参数封包类型	参数封包类型代码	说明	参数封包内容
防病毒	状态视图	VirusDetect_1.00	实时病毒扫描策略回显视图	见 A.3.4.1
		ActiveDefense_1.00	主动防御策略回显视图	见 A.3.4.1
		VirusScanTask _1.00	病毒扫描任务策略回显视图	见 A.3.4.1
		VirusScan_1.00	手动和快捷病毒扫描策略回显视图	见 A.3.4.1
	维护性操作	VirusScan_1.00	病毒扫描操作	见 A.3.5.2.2
网络隔离设备	设备参数	SDMI_1.00	系统接口参数	见 A.3.2.2
	状态视图	sys－info_1.00	设备系统信息视图	见 A.3.4.3.2.1
		net－info_1.00	网络状态信息视图，包括：网口信息、路由信息	见 A.3.4.3.2.2
		health－index_1.00	系统健康指数视图	见 A.3.4.3.2.4
		agent－info_1.00	代理接口信息视图	见 A.3.4.3.2.5
		reg－info_view_1.00	注册信息视图	见 A.3.4.3.6.1
		Isolation－policy_view_1.00	隔离策略视图	见 A.3.4.3.6.2
漏洞扫描设备	设备参数	SDMI_1.00	系统接口参数参数	见 A.3.2.2
		Interfaces_1.00	设备网络接口参数	见 A.3.2.3
	安全策略	Vulnerability_1.00	漏洞扫描策略	见 A.3.3.6
	状态视图	sys－info_1.00	设备系统信息视图	见 A.3.4.3.2.1
		net－info_1.00	网络状态信息视图，包括：网口信息、路由信息	见 A.3.4.3.2.2
		health－index_1.00	系统健康指数视图	见 A.3.4.3.2.4
		agent－info_1.00	代理接口信息视图	见 A.3.4.3.2.5
		Vulengin－info_1.00	漏洞扫描引擎视图	见 A.3.4.3.8.1
		VulnerabilityPolicy_1.00	漏洞扫描策略视图	见 A.3.4.2.2
		VulnerabilityList_1.00	漏洞扫描任务列表视图	见 A.3.4.3.8.2
		VulnerabilityResult_1.00	漏洞扫描结果视图	见 A.3.4.3.8.3
		VulInfo_1.00	漏洞信息视图	见 A.3.4.3.8.4
	维护性操作	Operation_1.00	通用维护性操作	见 A.3.5.1
		VulScan_1.00	漏洞扫描操作	见 A.3.5.2.3
授权管理	设备参数	SDMI_1.00	系统接口参数参数	见 A.3.2.2
数据库审计	设备参数	SDMI_1.00	系统接口参数参数	见 A.3.2.2
	安全策略	AUDIT_SERVER_CONF_MGM_1.00	数据库审计策略	见 A.3.3.5
	状态视图	sys－info_1.00	设备系统信息视图	见 A.3.4.3.2.1
		health－index_1.00	系统健康指数视图	见 A.3.4.3.2.4
		agent－info_1.00	代理接口信息视图	见 A.3.4.3.2.5
		AUDIT_SERVER_AUDIT_VIEW_1.00	审计节点审计管理视图	见 A.3.4.3.7.1
		AUDIT_SERVER_CONF_VIEW_1.00	审计节点配置管理视图	见 A.3.4.3.7.2

表 A.19(续)

设备类型	参数封包类型	参数封包类型代码	说明	参数封包内容
数据库审计	状态视图	ORACLE_INFO_VIEW_1.00	Oracle 信息视图	见 A.3.4.3.7.3
		SEC_SERVER_CONF_VIEW_1.00	访问控制节点配置管理视图	见 A.3.4.3.7.4
		SEC_SERVER_SEC_VIEW_1.00	访问控制节点安全管理视图	见 A.3.4.3.7.5
		SYS_VIEW_1.00	系统管理视图	见 A.3.4.3.7.6
补丁分发管理	设备参数	SDMI_1.00	系统接口参数参数	见 A.3.2.2
	安全策略	PATCH-DOWN-CONTROL_1.00	人工选择补丁分发策略	见 A.3.3.7.1
		PATCH-CLIENT-CONTROL_1.00	补丁自动分发策略	见 A.3.3.7.2
	状态视图	sys-info_1.00	设备系统信息视图	见 A.3.4.3.2.1
		health-index_1.00	系统健康指数视图	见 A.3.4.3.2.4
		agent-info_1.00	代理接口信息视图	见 A.3.4.3.2.5
		PATCH - CLIENT - CONTROL - VIEW_1.00	人工选择补丁分发策略视图	见 A.3.4.2.3
		PATCH - DOWN - CONTROL - VIEW_1.00	补丁自动分发策略视图	见 A.3.4.2.4
		Patch-Info_1.00	补丁安装信息视图	见 A.3.4.3.9.1
		host-list_1.00	主机列表视图	见 A.3.4.3.2.6
		Patch-List_1.00	补丁库列表视图	见 A.3.4.3.9.2
主机监控	设备参数	SDMI_1.00	系统接口参数	见 A.3.2.2
	安全策略	DevCtrl_2.00	外设控制策略	见 A.3.3.8.1
		HostUA_2.00	用户认证策略	见 A.3.3.8.2
		OCMonitor_2.00	外联监控策略	见 A.3.3.8.3
		IpAcl_1.00	IP 防火墙策略	见 A.3.3.2.1
		ContainerGuard_2.00	代理保护策略	见 A.3.3.8.4
	状态视图	sys-info_1.00	设备系统信息视图	见 A.3.4.3.2.1
		health-index_1.00	系统健康指数视图	见 A.3.4.3.2.4
		DevCtrl_2.00	外设控制策略回显视图	见 A.3.4.1
		HostUA_2.00	用户认证策略回显视图	见 A.3.4.1
		OCMonitor_2.00	外联监控策略回显视图	见 A.3.4.1
		IpAcl_1.00	IP 防火墙策略回显视图	见 A.3.4.1
		ContainerGuard_2.00	代理保护策略回显视图	见 A.3.4.1
		hw-hostgroup-list_1.00	主机组列表信息视图	见 A.3.4.3.10.1
		host-list_1.00	主机列表信息视图	见 A.3.4.3.2.6
		hw-usergroup-list_1.00	用户组列表信息视图	见 A.3.4.3.10.2
		hw-user-list_1.00	用户列表信息视图	见 A.3.4.3.10.3
		hw-server_stat_1.00	服务器统计信息视图	见 A.3.4.3.10.4

A.3.1.2 部分实现

在 SDMI::Policy::PolicyExecutor::fill 方法(见 A.1.2.6)被调用时，安全设备因为设备能力限制或

其他原因，无法完全执行某一参数封包内的全部内容，必须通过 extout 返回警告代码 W1001。

在 SDMI::Asset::AssetAgent::queryView 方法(见 A.1.2.6)被调用时，安全设备因为设备能力限制或其他原因，无法完全返回某一参数封包内的全部内容，仍必须返回该封包的完整 XML 标签格式和属性。无法填写内容的部分填写空字符串。

A.3.2 设备参数

A.3.2.1 封包格式

设备参数信息的参数封包遵循 SysConfigPack.dtd 的约束。SysConfigPack.dtd 的内容如下：

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ SysConfigPack.dtd －－>
<!ENTITY % CreateTime SYSTEM "CreateTime.dtd">
%CreateTime;
<!ELEMENT SysConfigPack (SysConfig)>
<!ELEMENT SysConfig (CreateTime, (SDMI | Interfaces | RouteTable))>
<!ATTLIST SysConfig
    type CDATA #REQUIRED
    version CDATA #REQUIRED
    description CDATA #IMPLIED
>
```

设备参数配置基本信息见表 A.20。

表 A.20 设备参数配置基本信息

参数名	类型	说明	允许取值
type	字符串	设备参数配置类型名	见 A.2.3.2 中对应设备配置参数类型代码的下划线字符前的部分
version	字符串	设备参数配置类型版本	见 A.2.3.2 中对应设备配置参数类型代码的下划线字符后的部分
description	字符串	描述	

A.3.2.2 系统接口参数

本参数用于 SDMI::Policy::PolicyExecutor::fill 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ SDMI_1.00.dtd －－>
<!ENTITY % SysConfigPack SYSTEM "SysConfigPack.dtd">
%SysConfigPack;
<!ELEMENT SDMI (Address, Address, Service, (AdditionalData＋))>
<!ENTITY % Address SYSTEM "Address.dtd">
%Address;
<!ELEMENT Service (port, protocol)>
<!ELEMENT port (#PCDATA)>
<!ELEMENT protocol (#PCDATA)>
<!ELEMENT AdditionalData (string | integer)>
<!ATTLIST AdditionalData
    meaning (event－enable | eps－limit | heartbeat－interval | with－rawdata) #REQUIRED
    type (integer | string) "string"
>
```

<!ELEMENT integer (#PCDATA)>
<!ELEMENT string (#PCDATA)>
系统接口参数说明见表 A.21。

表 A. 21　系统接口参数说明

参数名	允许取值	说明
xstf－path	见 A.2.4	设备标识
ipv4－addr	IP 地址	安全管理系统 IP 地址
port	0～65535	端口
protocol	固定为“TCP”	监听协议
meaning="event－enable"的 AdditionalData	yes/no	事件上报使能
meaning="eps－limit"的 AdditionalData	数字	事件流量限制(每秒事件数)
meaning="heartbeat－interval"的 AdditionalData	数字	心跳间隔，单位：秒
meaning="with－rawdata"的 AdditionalData	yes/no	是否上报原始事件，默认为 no

A. 3. 2. 3　设备网络接口参数

本参数用于 SDMI: : Policy: : PolicyExecutor: : fill 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ Interfaces_1.00.dtd －－>
<!ENTITY % SysConfigPack SYSTEM "SysConfigPack.dtd">
%SysConfigPack;
<!ENTITY % Address SYSTEM "Address.dtd">
%Address;
<!ENTITY % attvals.infmode "( access | trunk | bridge | dialup | route )">
<!ENTITY % attvals.infspeed "( 10 | 100 | 1000 | auto )">
<!ENTITY % attvals.infduplex "( half | full | auto )">
<!ENTITY % attvals.isadmin "( yes | no )">
<!ENTITY % attvals.ping "( enable | disable )">
<!ELEMENT Interfaces (Interface＋, AdditionalData*)>
<!ELEMENT Interface (Address*, Interface*)>
<!ATTLIST Interface
    name CDATA #REQUIRED
    mode %attvals.infmode; "route"
    device CDATA #IMPLIED
    mtu CDATA #IMPLIED
    speed %attvals.infspeed; "auto"
    duplex %attvals.infduplex; "auto"
    admin %attvals.isadmin; #IMPLIED
    ping %attvals.ping; #IMPLIED
    vlan－num CDATA #IMPLIED
>
<!ELEMENT AdditionalData ANY>
```

设备网络接口参数说明见表 A.22。

表 A. 22　设备网络接口参数说明

参数名	允许取值	说明
name	字符串	网络接口名称
mode	route/access/truck/bridge/dialup	工作模式，默认为 route
device	数字	硬件接口 ID
mtu	数字	最大传输单元，默认 1500
speed	10/100/1000/auto	网络接口传输速度，默认 auto
duplex	full/half/auto	网络接口工作方式，默认 auto
vlan－num	数字	VLAN 编号，如果 mode=truck 则需设置 vlan 标记
admin	yes/no	是否为管理口

A. 3. 2. 4　网络路由表参数

本参数用于 SDMI: :Policy: :PolicyExecutor: :fill 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ RouteTable_1.00.dtd －－>
<!ENTITY % SysConfigPack SYSTEM "SysConfigPack.dtd">
%SysConfigPack;
<!ENTITY % Address SYSTEM "Address.dtd">
%Address;
<!ELEMENT RouteTable (Route*, AdditionalData*)>
<!ELEMENT Source (Address)>
<!ELEMENT Target (Address)>
<!ELEMENT Gateway (Address)>
<!ELEMENT Route (Source?, Target?, Gateway)>
<!ATTLIST Route
    interface CDATA #REQUIRED
    metric CDATA #IMPLIED
>
<!ELEMENT AdditionalData ANY>
```

设备网络接口参数说明见表 A.23。

表 A. 23　设备网络接口参数说明

参数名	允许取值	说明
interface	必须与设备网络接口配置中对应网络接口的 name 参数一致	见 A.3.2.3
metric	数字	跃点计数

A. 3. 3　安全策略

A. 3. 3. 1　封包格式

安全策略的参数封包遵循 PolicyPack.dtd 的约束。PolicyPack.dtd 的内容如下：

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ PolicyPack.dtd －－>
<!ENTITY % CreateTime SYSTEM "CreateTime.dtd">
%CreateTime;
```

```
<!ELEMENT PolicyPack (Policy)>
<!ATTLIST Policy
    type CDATA #REQUIRED
    version CDATA #REQUIRED
    description CDATA #IMPLIED
    mode (transient | persistent) "persistent"
>
```

安全策略基本信息见表 A.24。

表 A. 24　安全策略基本信息

参数名	类型	说明	允许取值
type	字符串	安全策略类型名	见 A.2.3.3 中对应安全策略类型代码的下划线字符前的部分
version	字符串	安全策略类型版本	见 A.2.3.3 中对应安全策略类型代码的下划线字符后的部分
description	字符串	描述	
mode	字符串	安全策略执行模式	transient/persistent

A. 3. 3. 2　防火墙

A. 3. 3. 2. 1　IP 访问控制

本安全策略用于 SDMI::Policy::PolicyExecutor::fill 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ IpAcl_1.00.dtd －－>
<!ENTITY % PolicyPack SYSTEM "PolicyPack.dtd">
%PolicyPack;
<!ENTITY % Address SYSTEM "Address.dtd">
%Address;
<!ELEMENT Policy (CreateTime, IpAcl)>
<!ENTITY % attvals.acldirect "( inbound | outbound | both )">
<!ENTITY % attvals.hpdirect "( bidirect | statgoto | statback | nostatgoto | nostatback )">
<!ENTITY % attvals.yesno "( yes | no )">
<!ELEMENT Action (#PCDATA)>
<!ATTLIST Action
    category CDATA #FIXED "firewall"
>
<!ELEMENT HyperProtocol (Source?, Target)>
<!ATTLIST HyperProtocol
    name CDATA #REQUIRED
    direct %attvals.hpdirect; #REQUIRED
    major %attvals.yesno; #REQUIRED
    description CDATA #REQUIRED
>
<!ELEMENT HyperService (HyperProtocol＋)>
<!ATTLIST HyperService
    name CDATA #REQUIRED
```

```
    description CDATA #REQUIRED
>
<!ELEMENT IpAcl (IpAclRule*, AdditionalData*)>
<!ELEMENT IpAclRule (Source?, Target?, HyperService?, Action, TimeScope?, TimeCycle?)>
<!ATTLIST IpAclRule
    log %attvals.yesno; "no"
    interface CDATA #IMPLIED
    direction %attvals.acldirect; #IMPLIED
>
<!ELEMENT Service (port?, portlist?, protocol)>
<!ELEMENT Source (Address+ | Service | User)>
<!ELEMENT Target (Address | Service)>
<!ELEMENT TimeCycle (minute, hour, day－of－week, month)>
<!ELEMENT TimeScope (TimeSpan+)>
<!ELEMENT TimeSpan (start－time, end－time?)>
<!ATTLIST TimeSpan
    type CDATA #REQUIRED
>
<!ELEMENT User (UserId+)>
<!ELEMENT UserId (name)>
<!ELEMENT day－of－week (#PCDATA)>
<!ELEMENT end－time (hour)>
<!ELEMENT hour (#PCDATA)>
<!ELEMENT minute (#PCDATA)>
<!ELEMENT month (#PCDATA)>
<!ELEMENT name (#PCDATA)>
<!ELEMENT port (#PCDATA)>
<!ELEMENT portlist (#PCDATA)>
<!ELEMENT protocol (#PCDATA)>
<!ELEMENT start－time (day－of－week | hour)>
<!ELEMENT AdditionalData ANY>
```

地址转换策略参数见表 A.25。

表 A. 25　地址转换策略参数说明

参数名	允许取值	说明
direct	bidirect/statgoto/statback/nostatgoto/nostatback	协议的方向
Action	deny/accept/reject/accounting/skip/continue/encrypt	采取的措施

A. 3. 3. 2. 2　地址转换

本安全策略用于 SDMI: : Policy: : PolicyExecutor: : fill 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ NAT_1.00.dtd －－>
<!ENTITY % PolicyPack SYSTEM "PolicyPack.dtd">
%PolicyPack;
```

```
<!ENTITY % Address SYSTEM "Address.dtd">
%Address;
<!ELEMENT Policy (CreateTime, NAT)>
<!ELEMENT NAT (NATRule*, AdditionalData*)>
<!ELEMENT NATOriginal (Source, Target)>
<!ELEMENT NATRule (NATOriginal, NATTranslated)>
<!ELEMENT NATTranslated (Source, Target)>
<!ELEMENT Service (portlist?, port?, protocol)>
<!ELEMENT Source (Address?)>
<!ELEMENT Target (Address?, Service?)>
<!ELEMENT port (#PCDATA)>
<!ELEMENT portlist (#PCDATA)>
<!ELEMENT protocol (#PCDATA)>
<!ELEMENT AdditionalData ANY>
```

A.3.3.3 入侵检测

本安全策略用于 SDMI::Policy::PolicyExecutor::fill 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- IDS_1.00.dtd -->
<!ENTITY % PolicyPack SYSTEM "PolicyPack.dtd">
%PolicyPack;
<!ENTITY % Address SYSTEM "Address.dtd">
%Address;
<!ENTITY % AdditionalData SYSTEM "AdditionalData.dtd">
%AdditionalData;
<!ELEMENT Policy (CreateTime, IDS)>
<!ENTITY % attvals.fusecat "
    (sip_dip | sip | dip | count | snet_dip | dnet_sip | sip_sport | sip_dport | dip_sport | dip_dport |
snet_sport | snet_dport | dnet_sport | dnet_dport)
">
<!ELEMENT Action (#PCDATA)>
<!ATTLIST Action
    category CDATA #FIXED "ids"
>
<!ELEMENT Assessment (Impact)>
<!ELEMENT IDS (IDSRule*)>
<!ELEMENT IDSRule (Source?, Target?, Action, Assessment, AdditionalData)>
<!ATTLIST IDSRule
    ident CDATA #REQUIRED
    name CDATA #REQUIRED
    fuse %attvals.fusecat; #REQUIRED
>
<!ELEMENT Impact (#PCDATA)>
<!ELEMENT Source (Address*)>
```

<!ELEMENT Target (Address*)>

设备网络接口参数说明见表 A.26。

表 A.26　设备网络接口参数说明表

参数名	允许取值	说明
ident	字符串	检测规则的 ID
name	字符串	检测规则名
fuse	字符串	合并方式
category="ids"的 Action	log/alarm/block	处理方式
Impact	info/low/medium/high	事件级别

A.3.3.4　防病毒

A.3.3.4.1　实时病毒检测

本安全策略用于 SDMI::Policy::PolicyExecutor::fill 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ VirusDetect_1.00.dtd －－>
<!ENTITY % PolicyPack SYSTEM "PolicyPack.dtd">
%PolicyPack;
<!ELEMENT Policy (CreateTime, VirusDetect＋)>
<!ELEMENT VirusDetect (Action＋, FileType?, FileFormat?, UnknownVirusType?, pop3?, smtp?)>
<!ATTLIST VirusDetect
    category (file | email | web) #REQUIRED
    enable (yes | no) #REQUIRED
>
<!ELEMENT Action (#PCDATA)>
<!ATTLIST Action
    category CDATA #FIXED "antivirus"
    assert (default | fail) #REQUIRED
>
<!ELEMENT FileType (#PCDATA)>
<!ATTLIST FileType
    option (all | custom) #REQUIRED
>
<!ELEMENT FileFormat (#PCDATA)>
<!ELEMENT UnknownVirusType (#PCDATA)>
<!ELEMENT pop3 (port＋)>
<!ELEMENT smtp (port＋)>
<!ELEMENT port (#PCDATA)>
<!ATTLIST port
    enable (yes | no) #REQUIRED
>
```

A.3.3.4.2　主动防御

本安全策略用于 SDMI::Policy::PolicyExecutor::fill 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ ActiveDefense_1.00.dtd －－>
<!ENTITY % PolicyPack SYSTEM "PolicyPack.dtd">
%PolicyPack;
<!ELEMENT Policy (CreateTime, ActiveDefense＋)>
<!ELEMENT ActiveDefense EMPTY>
<!ATTLIST ActiveDefense
    category (System | AppAccessControl | AppProtection | AppStartupControl | SelfProtection)
#REQUIRED
    enable (yes | no) #REQUIRED
>
```

A. 3. 3. 4. 3　定时病毒扫描任务

本安全策略用于 SDMI: : Policy: : PolicyExecutor: : fill 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ VirusScanTask_1.00.dtd －－>
<!ENTITY % PolicyPack SYSTEM "PolicyPack.dtd">
%PolicyPack;
<!ELEMENT Policy (CreateTime, VirusScanTask)>
<!ELEMENT VirusScanTask (TimeCycle, Action＋, FileType, FileFormat, UnknownVirusType,
AdditionalData)>
<!ELEMENT TimeCycle (minute, hour)>
<!ELEMENT minute (#PCDATA)>
<!ELEMENT hour (#PCDATA)>
<!ELEMENT Action (#PCDATA)>
<!ATTLIST Action
    category CDATA #FIXED "antivirus"
    assert (default | fail) #REQUIRED
>
<!ELEMENT FileType (#PCDATA)>
<!ATTLIST FileType
    option (all | custom) #REQUIRED
>
<!ELEMENT FileFormat (#PCDATA)>
<!ELEMENT UnknownVirusType (#PCDATA)>
<!ELEMENT AdditionalData (string)>
<!ATTLIST AdditionalData
    meaning CDATA #FIXED "target"
    type (string) "string"
>
<!ELEMENT string (#PCDATA)>
```

A. 3. 3. 4. 4　手动/快捷病毒扫描

本安全策略用于 SDMI: : Policy: : PolicyExecutor: : fill 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
```

```
<!-- VirusScan_1.00.dtd -->
<!ENTITY % PolicyPack SYSTEM "PolicyPack.dtd">
%PolicyPack;
<!ELEMENT Policy (CreateTime, VirusScan+)>
<!ELEMENT VirusScan (Action*, FileType?, FileFormat?, UnknownVirusType?)>
<!ATTLIST VirusScan
    category (demand | manual | shortcut) #REQUIRED
>
<!ELEMENT Action (#PCDATA)>
<!ATTLIST Action
    category CDATA #FIXED "antivirus"
    assert (default | fail) #IMPLIED
>
<!ELEMENT FileType (#PCDATA)>
<!ATTLIST FileType
    option (all | custom) #REQUIRED
>
<!ELEMENT FileFormat (#PCDATA)>
<!ELEMENT UnknownVirusType (#PCDATA)>
```

A.3.3.5 数据库审计

本安全策略用于 SDMI::Policy::PolicyExecutor::fill 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- AUDIT_SERVER_CONF_MGM_1.00.dtd -->
<!ENTITY % PolicyPack SYSTEM "PolicyPack.dtd">
%PolicyPack;
<!ELEMENT Policy (CreateTime, NODE+)>
<!ELEMENT AUDIT (AU_USER, INSTANCE, SCHEMA, OBJECT, EVENT, RESULT)>
<!ELEMENT AU_USER (#PCDATA)>
<!ELEMENT COLUMN_PRIV (string*)>
<!ATTLIST COLUMN_PRIV
    NAME CDATA #REQUIRED
    VALUE CDATA #REQUIRED
>
<!ELEMENT ROLE_USER EMPTY>
<!ATTLIST ROLE_USER
    ROLE_NAME CDATA #REQUIRED
    USER_NAME CDATA #REQUIRED
>
<!ELEMENT CONSTRAIN EMPTY>
<!ATTLIST CONSTRAIN
    VALUE CDATA #REQUIRED
>
<!ELEMENT DBA (#PCDATA)>
```

```
<!ELEMENT DES (#PCDATA)>
<!ELEMENT EVENT (#PCDATA)>
<!ELEMENT GLOBAL_PRIV EMPTY>
<!ATTLIST GLOBAL_PRIV
    VALUE CDATA #REQUIRED
>
<!ELEMENT INSTANCE (#PCDATA | DBA | INSTANCE_NAME | PWD | USER) *>
<!ELEMENT INSTANCE_NAME (#PCDATA)>
<!ELEMENT IS_OPEN (#PCDATA)>
<!ELEMENT IS_START (#PCDATA)>
<!ELEMENT NODE (IS_START?, IS_OPEN?, PORT?, USER?, PWD?, DES?, AUDIT*,
ROLE*,ROLE_USER*, INSTANCE*)>
<!ATTLIST NODE
    IP CDATA #REQUIRED
    TYPE CDATA #REQUIRED
>
<!ELEMENT OBJECT (#PCDATA)>
<!ELEMENT PORT (#PCDATA)>
<!ELEMENT PRIV (GLOBAL_PRIV, TABLE_PRIV)>
<!ELEMENT PWD (#PCDATA)>
<!ELEMENT RESULT (#PCDATA)>
<!ELEMENT ROLE (INSTANCE, ROLE_NAME, PRIV)>
<!ELEMENT ROLE_NAME (#PCDATA)>
<!ELEMENT SCHEMA (#PCDATA)>
<!ELEMENT TABLE_PRIV (COLUMN_PRIV, CONSTRAIN)>
<!ATTLIST TABLE_PRIV
    NAME CDATA #REQUIRED
    VALUE CDATA #REQUIRED
>
<!ELEMENT USER (#PCDATA)>
```

数据库审计策略参数说明见表 A.27。

表 A.27　数据库审计策略参数说明表

参数名	允许取值	说明
AU_USER	字符串	审计用户
INSTANCE	字符串	Oracle 实例名
SCHEMA	字符串	模式名
OBJECT	字符串	对象名
EVENT	字符串	事件类型
RESULT	字符串	结果类型
ROLE_NAME	字符串	角色名
GLOBAL_PRIV	字符串	全局权限

表 A. 27(续)

参数名	允许取值	说明
TABLE_PRIV	字符串	表级权限
COLUMN_PRIV	字符串	列级权限
CONSTRAIN	字符串	行级约束
INSTANCE_NAME	字符串	Oracle 实例名

A. 3. 3. 6 漏洞扫描

本安全策略用于 SDMI: : Policy: : PolicyExecutor: : fill 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ Vulnerability_1.00.dtd －－>
<!ENTITY % PolicyPack SYSTEM "PolicyPack.dtd">
%PolicyPack;
<!ELEMENT Policy (CreateTime, Vulnerability)>
<!ELEMENT Vulnerability (scan_task＋)>
<!ELEMENT scan_task (scan_name, ip_scope, scan_type, scan_unit, cycle, VulPolicy, ScanPara)>
<!ELEMENT scan_name (#PCDATA)>
<!ELEMENT ip_scope (#PCDATA)>
<!ELEMENT scan_type (#PCDATA)>
<!ELEMENT scan_unit (#PCDATA)>
<!ELEMENT cycle (#PCDATA)>
<!ELEMENT VulPolicy (vul)>
<!ATTLIST VulPolicy
    name CDATA #REQUIRED
    description CDATA #REQUIRED
>
<!ELEMENT vul (#PCDATA)>
<!ELEMENT ScanPara (para＋)>
<!ELEMENT para (#PCDATA | protocol | scan_scope | scan_timeout | para_name | para_value |
notify_email | notify_ip | notify_time | notify_type | notify_flag | snmp_ip | snmp_password | snmp_port |
snmp_risk) *>
<!ATTLIST para name (scan_thread_num | scan_host_num | vul_scan_time | scan_type_0 | scan_type_1 |
scan_type_2 | scan_type_3 | port | deepscan | hidescan | notify | snmp_notify) "scan_thread_num">
<!ELEMENT notify_email (#PCDATA)>
<!ELEMENT notify_flag (#PCDATA)>
<!ELEMENT notify_ip (#PCDATA)>
<!ELEMENT notify_time (#PCDATA)>
<!ELEMENT notify_type (#PCDATA)>
<!ELEMENT para_name (#PCDATA)>
<!ELEMENT para_value (#PCDATA)>
<!ELEMENT protocol (#PCDATA)>
<!ELEMENT scan_scope (#PCDATA)>
<!ELEMENT scan_timeout (#PCDATA)>
```

<!ELEMENT snmp_ip (#PCDATA)>
<!ELEMENT snmp_password (#PCDATA)>
<!ELEMENT snmp_port (#PCDATA)>
<!ELEMENT snmp_risk (#PCDATA)>
递进扫描参数见表 A.28。
隐蔽扫描参数见表 A.29。

表 A.28 递进扫描参数

参数名	说明	允许取值
SMB account:	SMB 用户名	字符串
SMB password:	SMB 密码	字符串
SMB domain (optional):	SMB 域(可选)	字符串
Never send SMB credentials in clear text	不使用明文发送 SMB 认证	yes|no
Only use NTLMv2	只使用 NTLMv2	yes|no
FTP account:	FTP 用户名	字符串
FTP password (sent in clear):	FTP 密码(明文发送)	字符串
FTP writeable directory:	FTP 可写的路径	字符串
HTTP account:	HTTP 用户名	字符串
HTTP password (sent in clear):	HTTP 密码(明文发送)	字符串
SNMP community (sent in clear):	SNMP community(明文发送)	字符串
TELNET account:	TELNET 用户名	字符串
TELNET password (sent in clear):	TELNET 密码(明文发送)	字符串
DB2 account:	DB2 用户名	字符串
DB2 password:	DB2 密码	字符串
ORACLE account:	ORACLE 用户名	字符串
ORACLE password:	ORACLE 密码	字符串
SYBASE account:	SYBASE 用户名	字符串
SYBASE password (sent in clear):	SYBASE 密码(明文发送)	字符串
POP2 account:	POP2 用户名	字符串
POP2 password (sent in clear):	POP2 密码(明文发送)	字符串
POP3 account:	POP3 用户名	字符串
POP3 password (sent in clear):	POP3 密码(明文发送)	字符串
NNTP account:	NNTP 用户名	字符串
NNTP password (sent in clear):	NNTP 密码(明文发送)	字符串
IMAP account:	IMAP 用户名	字符串
IMAP password (sent in clear):	IMAP 密码(明文发送)	字符串
Third party domain:	SMTP 设置：第三方域	字符串
From address:	SMTP 设置：发件人	字符串
To address:	SMTP 设置：收件人	字符串
Start page:	WEB 镜像起始页面	字符串
Send POST requests	用 POST 方法检测	yes|no

表 A. 29　隐蔽扫描参数

参数名	说明	允许取值
HTTP	HTTP 用户代理	字符串
Use	使用 HTTP 头	字符串
URL	URL 编码	none|Hex|UTF－16（double byte）| UTF－16（MS %u）|Incorrect UTF－8
Double	双斜杆替换	字符串
Reverse	反向遍历	none|Basic|Long URL
Absolute	绝对的 URI 类型	none|file|gopher|http
Absolute	绝对的 URI 主机	none|host name|host IP|random name|random IP
Self－reference	/./目录插入	字符串
Dos/Windows	使用\代替/	字符串
Null	NULL 方法	字符串
TAB	TAB 分割	字符串
HTTP/0.9	HTTP/0.9 请求	字符串
Premature	过早结束 URL	字符串
CGI.pm	CGI.pm 分号分离	字符串
Parameter	参数隐藏	字符串
Force	强制协议字符串	字符串
Random	随机大小写	字符串
Send	发送伪造的 RST	字符串
TCP	TCP 逃避技术	none|split|网络包插入|小的 ttl

A. 3. 3. 7　补丁分发

A. 3. 3. 7. 1　人工选择补丁分发

本安全策略用于 SDMI: : Policy: : PolicyExecutor: : fill 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ PATCH－DOWN－CONTROL_1.00.dtd －－>
<!ENTITY % PolicyPack SYSTEM "PolicyPack.dtd">
%PolicyPack;
<!ENTITY % attvals.yesno "( yes | no )">
<!ELEMENT Policy (CreateTime, NODE＋)>
<!ELEMENT NODE (Repscript)>
<!ATTLIST NODE
    IP CDATA #REQUIRED
    CLASS CDATA #FIXED "PATCH－DOWN－CONTROL"
>
<!ELEMENT Repscript (item)>
<!ATTLIST Repscript
    PolicyName CDATA #REQUIRED
```

```
    StartPolicy %attvals.yesno; #REQUIRED
    PolicyStartTime CDATA #REQUIRED
    PolicyEndTime CDATA #REQUIRED
    InvalidWeekDay (0 | 1 | 2 | 3 | 4 | 5 | 6) #REQUIRED
    DBT1 CDATA #REQUIRED
    DET1 CDATA #REQUIRED
    DBT2 CDATA #REQUIRED
    DET2 CDATA #REQUIRED
    DBT3 CDATA #REQUIRED
    DET3 CDATA #REQUIRED
    ControlRegionMode CDATA #REQUIRED
    NetValidMode %attvals.yesno; #REQUIRED
    UserValidMode %attvals.yesno; #REQUIRED
    ExceptUser CDATA #REQUIRED
    Remark CDATA #REQUIRED
    FourceUseFatherDeal %attvals.yesno; #REQUIRED
>
<!ELEMENT item (Prompt*, CheckConfig, Retry)>
<!ATTLIST item
    FileName CDATA #REQUIRED
    CmdArgv CDATA #REQUIRED
    RunHidden %attvals.yesno; #REQUIRED
    RunProcLevel CDATA #REQUIRED
>
<!ELEMENT Prompt (#PCDATA)>
<!ATTLIST Prompt
    type (1 | 2) #REQUIRED
    enable %attvals.yesno; #REQUIRED
>
<!ELEMENT CheckConfig ((Week, Time) | Interval)>
<!ATTLIST CheckConfig
    CheckType (0 | 1 | 2 | 3) #REQUIRED
>
<!ELEMENT Week (#PCDATA)>
<!ELEMENT Time (#PCDATA)>
<!ELEMENT Interval (#PCDATA)>
<!ELEMENT Retry EMPTY>
<!ATTLIST Retry
    enable %attvals.yesno; #REQUIRED
    RetryCount CDATA #REQUIRED
    RetryTime CDATA #REQUIRED
>
```

人工选择补丁分发策略参数说明见表 A.30。

表 A.30　人工选择补丁分发策略参数说明

参数名	允许取值	说明
PolicyName	字符串	策略名称
StartPolicy	yes/no	策略是否启用
PolicyStartTime	IDMEF 时间戳格式	策略存活时间范围(开始时间)
PolicyEndTime	IDMEF 时间戳格式	策略存活时间范围(结束时间)
InvalidWeekDay	0～6	策略无效工作日，0 代表周日，1 至 6 分别代表周一至周六
DBT1	字符串	策略无效时间段 1(开始时间)
DET1	字符串	策略无效时间段 1(结束时间)
DBT2	字符串	策略无效时间段 2(开始时间)
DET2	字符串	策略无效时间段 2(结束时间)
DBT3	字符串	策略无效时间段 3(开始时间)
DET3	字符串	策略无效时间段 3(结束时间)
ControlRegionMode	字符串	策略级联区域的选择
NetValidMode	yes/no	策略有效网络
UserValidMode	yes/no	策略有效用户
ExceptUser	字符串	例外用户
Remark	字符串	备注信息
FourceUseFatherDeal	yes/no	强制使用父对象策略
FileName	字符串	补丁下载路径(含补丁名)
CmdArgv	字符串	命令行参数
RunHidde	yes/no	是否后台运行
RunProcLevel	数字	运行优先级
CheckType	数字	检测方式，0 为不检测，1 为启动时检测，2 为定时检测，3 为周期性检测
Week	0～6	检测工作日，0 代表周日，1 至 6 分别代表周一至周六。当且仅当 CheckType＝2 时有效。
Time	mm:ss 的格式	检测时间。当且仅当 CheckType＝2 时有效。
Interval	数字	间隔时间，单位：分。当且仅当 CheckType＝3 时有效。
Retry	yes/no	下载失败是否重试
RetryCount	数字	重试次数
RetryTime	数字	重试间隔，单位：分

A.3.3.7.2　补丁自动分发

本安全策略用于 SDMI::Policy::PolicyExecutor::fill 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- PATCH-CLIENT-CONTROL_1.00.dtd -->
<!ENTITY % PolicyPack SYSTEM "PolicyPack.dtd">
%PolicyPack;
<!ENTITY % attvals.yesno "( yes | no )">
```

```
<!ELEMENT Policy (CreateTime, NODE+)>
<!ELEMENT NODE (Repscript)>
<!ATTLIST NODE
    IP CDATA #REQUIRED
    CLASS CDATA #FIXED "PATCH-CLIENT-CONTROL"
>
<!ELEMENT Repscript (item)>
<!ATTLIST Repscript
    PolicyName CDATA #REQUIRED
    StartPolicy %attvals.yesno; #REQUIRED
    PolicyVersion CDATA #REQUIRED
    PolicyStartTime CDATA #REQUIRED
    PolicyEndTime CDATA #REQUIRED
    InvalidWeekDay CDATA #REQUIRED
    DBT1 CDATA #REQUIRED
    DET1 CDATA #REQUIRED
    DBT2 CDATA #REQUIRED
    DET2 CDATA #REQUIRED
    DBT3 CDATA #REQUIRED
    DET3 CDATA #REQUIRED
    ControlRegionMode CDATA #REQUIRED
    NetValidMode %attvals.yesno; #REQUIRED
    UserValidMode %attvals.yesno; #REQUIRED
    ExceptUser CDATA #REQUIRED
    GatewayValidMode %attvals.yesno; #REQUIRED
    ExceptGateway CDATA #REQUIRED
    Remark CDATA #REQUIRED
    FourceUseFatherDeal %attvals.yesno; #REQUIRED
>
<!ELEMENT item (Classes, Prompt*, CheckConfig, Retry)>
<!ATTLIST item
    PatchLevel CDATA #REQUIRED
    CmdArgv CDATA #REQUIRED
    RunHidden CDATA #REQUIRED
    RunProcLevel CDATA #REQUIRED
    ReStartComputer CDATA #REQUIRED
    ReStartAndInfo %attvals.yesno; #REQUIRED
>
<!ELEMENT Classes (Class+)>
<!ELEMENT Class EMPTY>
<!ATTLIST Class
    type CDATA #REQUIRED
    enable %attvals.yesno; #REQUIRED
```

```
>
<!ELEMENT Prompt (#PCDATA)>
<!ATTLIST Prompt
    type (1 | 2) #REQUIRED
    enable %attvals.yesno; #REQUIRED
>
<!ELEMENT CheckConfig ((Week, Time) | Interval)>
<!ATTLIST CheckConfig
    CheckType (0 | 1 | 2 | 3) #REQUIRED
>
<!ELEMENT Week (#PCDATA)>
<!ELEMENT Time (#PCDATA)>
<!ELEMENT Interval (#PCDATA)>
<!ELEMENT Retry EMPTY>
<!ATTLIST Retry
    enable %attvals.yesno; #REQUIRED
    RetryCount CDATA #REQUIRED
    RetryTime CDATA #REQUIRED
>
```

补丁自动分发策略参数说明见表 A.31。

表 A.31 补丁自动分发策略参数说明

参数名	允许取值	说明
PolicyVersion	字符串	策略版本
GatewayValidMode	字符串	策略有效网关
ExceptGateway	字符串	例外网关
PatchLevel	数字	安装补丁的级别
ReStartComputer	数字	补丁安装完成后要求重启计算机时的操作
ReStartAndInfo	yes/no	重启后是否显示补丁安装情况
其他		见 A.3.3.7.1

A.3.3.8 主机监控

A.3.3.8.1 外设控制

本安全策略用于 SDMI::Policy::PolicyExecutor::fill 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- DevCtrl_2.00.dtd -->
<!ENTITY % PolicyPack SYSTEM "PolicyPack.dtd">
%PolicyPack;
<!ENTITY % attvals.ctrlmode "(Enable | Disable | ReadOnly | WriteOnly)">
<!ELEMENT Policy (CreateTime, StorageDeviceRule, OtherDeviceRule, LogRule,
ThirdPartySupportRule)>
<!ELEMENT StorageDeviceRule (CdRom, Floppy, Usb, IEEE1394)>
<!ELEMENT CdRom EMPTY>
```

```
<!ATTLIST CdRom
    ControlMode %attvals.ctrlmode; #REQUIRED
>
<!ELEMENT Floppy EMPTY>
<!ATTLIST Floppy
    ControlMode %attvals.ctrlmode; #REQUIRED
>
<!ELEMENT Usb EMPTY>
<!ATTLIST Usb
    ControlMode %attvals.ctrlmode; #REQUIRED
>
<!ELEMENT IEEE1394 EMPTY>
<!ATTLIST IEEE1394
    ControlMode %attvals.ctrlmode; #REQUIRED
>
<!ELEMENT OtherDeviceRule (SerialPort, Printer)>
<!ELEMENT SerialPort EMPTY>
<!ATTLIST SerialPort
    ControlMode %attvals.ctrlmode; #REQUIRED
>
<!ELEMENT Printer EMPTY>
<!ATTLIST Printer
    ControlMode %attvals.ctrlmode; #REQUIRED
>
<!ELEMENT LogRule (WriteLog)>
<!ELEMENT WriteLog (#PCDATA)>
<!ELEMENT ThirdPartySupportRule (YangDunUsb)>
<!ELEMENT YangDunUsb (#PCDATA)>
```

A.3.3.8.2 用户认证

本安全策略用于 SDMI::Policy::PolicyExecutor::fill 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ HostUA_2.00.dtd －－>
<!ENTITY % PolicyPack SYSTEM "PolicyPack.dtd">
%PolicyPack;
<!ELEMENT Policy (CreateTime, AuthRule)>
<!ELEMENT AuthRule (#PCDATA)>
<!ATTLIST AuthRule
    OnlineMode (yes | no) #REQUIRED
    DisableGuest (yes | no) #REQUIRED
    Type (AUTHUSERNAME | AUTHUSBKEY) #REQUIRED
>
```

A.3.3.8.3 外联监控

本安全策略用于 SDMI::Policy::PolicyExecutor::fill 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ OCMonitor_2.00.dtd －－>
<!ENTITY % PolicyPack SYSTEM "PolicyPack.dtd">
%PolicyPack;
<!ELEMENT Policy (CreateTime, IsLog, DeviceList)>
<!ELEMENT IsLog (#PCDATA)>
<!ELEMENT DeviceList (DeviceRule*)>
<!ATTLIST DeviceList
    Num CDATA #REQUIRED
>
<!ELEMENT DeviceRule (DeviceType, IsLegal, Comment?)>
<!ELEMENT DeviceType (#PCDATA)>
<!ELEMENT IsLegal (#PCDATA)>
<!ELEMENT Comment (#PCDATA)>
```

A.3.3.8.4 IP 防火墙

见 A.3.3.2.1。

A.3.3.8.5 代理保护

本安全策略用于 SDMI::Policy::PolicyExecutor::fill 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ ContainerGuard_2.00.dtd －－>
<!ENTITY % PolicyPack SYSTEM "PolicyPack.dtd">
%PolicyPack;
<!ENTITY % attvals.yesno "( yes | no )">
<!ELEMENT Policy (CreateTime, SafeMode, ModifyIp, AddUser, ForceMode)>
<!ELEMENT SafeMode (#PCDATA)>
<!ATTLIST SafeMode
    enable %attvals.yesno; #REQUIRED
>
<!ELEMENT ModifyIp (#PCDATA)>
<!ATTLIST ModifyIp
    enable %attvals.yesno; #REQUIRED
>
<!ELEMENT AddUser (#PCDATA)>
<!ATTLIST AddUser
    enable %attvals.yesno; #REQUIRED
>
<!ELEMENT ForceMode (#PCDATA)>
<!ATTLIST ForceMode
    enable %attvals.yesno; #REQUIRED
>
```

A.3.4 状态视图

A.3.4.1 安全策略回显视图

本类视图用于 SDMI::Asset::AssetAgent::queryView 方法，见 A.1.2.6。

安全策略回显视图的 XML 采用与安全策略完全一致的形式，即参数封包格式也采用安全策略封包一致的形式，见 A.3.3。

目前已有的安全策略回显视图见表 A.32。

表 A.32 安全策略回显视图列

类型代码	说明	参数封包内容
NAT_1.00	地址转换策略回显视图	见 A.3.3.2.2
IDS_1.00	入侵检测策略回显视图	见 A.3.3.3
VirusDetect_1.00	实时病毒检测策略回显视图	见 A.3.3.4.1
ActiveDefense_1.00	主动防御策略回显视图	见 A.3.3.4.2
VirusScanTask _1.00	定时病毒扫描任务策略回显视图	见 A.3.3.4.3
VirusScan_1.00	手动/快捷病毒扫描策略回显视图	见 A.3.3.4.4
DevCtrl_2.00	外设控制策略回显视图	见 A.3.3.8.1
HostUA_2.00	用户认证策略回显视图	见 A.3.3.8.2
OCMonitor_2.00	外联监控策略回显视图	见 A.3.3.8.3
IpAcl_1.00	IP 防火墙策略回显视图	见 A.3.3.2.1
ContainerGuard_2.00	代理保护策略回显视图	见 A.3.3.8.4

A.3.4.2 安全策略视图

A.3.4.2.1 封包格式

安全策略视图的参数封包遵循 ViewData_Policy.dtd 的约束。ViewData_Policy.dtd 的内容如下：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- ViewData_Policy.dtd -->
<!ELEMENT ViewData (CreateTime, AdditionalData)>
<!ATTLIST ViewData
    name NMTOKEN #REQUIRED
    version NMTOKEN #REQUIRED
>
<!ENTITY % AdditionalData SYSTEM "AdditionalData.dtd">
%AdditionalData;
```

安全策略视图基本信息见表 A.33。

表 A.33 安全策略视图基本信息

参数名	类型	说明	允许取值
name	字符串	状态视图类型名	见 A.2.3.4 中对应状态视图类型代码的下划线字符前的部分
version	字符串	状态视图类型版本	见 A.2.3.4 中对应状态视图类型代码的下划线字符后的部分

A.3.4.2.2 漏洞扫描策略视图

本视图用于 SDMI::Asset::AssetAgent::queryView 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- VulnerabilityPolicy_1.00.dtd -->
<!ENTITY % ViewData SYSTEM "ViewData_Policy.dtd">
%ViewData;
```

```
<!ENTITY % Vulnerability SYSTEM "Vulnerability_1.00.dtd">
%Vulnerability;
<!ELEMENT xml (Vulnerability)>
```

A.3.4.2.3 人工选择补丁分发策略视图

本视图用于 SDMI::Asset::AssetAgent::queryView 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ PATCH－DOWN－CONTROL－VIEW_1.00.dtd －－>
<!ENTITY % ViewData SYSTEM "ViewData_Policy.dtd">
%ViewData;
<!ENTITY % NODE SYSTEM "PATCH－DOWN－CONTROL_1.00.dtd">
%NODE;
<!ELEMENT xml (NODE*)>
```

A.3.4.2.4 补丁自动分发策略视图

本视图用于 SDMI::Asset::AssetAgent::queryView 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ PATCH－CLIENT－CONTROL－VIEW_1.00.dtd －－>
<!ENTITY % ViewData SYSTEM "ViewData_Policy.dtd">
%ViewData;
<!ENTITY % NODE SYSTEM "PATCH－CLIENT－CONTROL_1.00.dtd">
%NODE;
<!ELEMENT xml (NODE*)>
```

A.3.4.3 普通状态视图

A.3.4.3.1 封包格式

除安全策略回显视图和安全策略视图外的所有状态视图，其参数封包遵循 ViewData.dtd 的约束。ViewData.dtd 的内容如下：

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ ViewData.dtd －－>
<!ELEMENT ViewData (CreateTime, AdditionalData)>
<!ATTLIST ViewData
    name NMTOKEN #REQUIRED
    version NMTOKEN #REQUIRED
>
<!ENTITY % CreateTime SYSTEM "CreateTime.dtd">
%CreateTime;
<!ENTITY % AdditionalData SYSTEM "AdditionalData.dtd">
%AdditionalData;
```

状态视图基本信息见表 A.34。

表 A.34 状态视图基本信息

参数名	类型	说明	允许取值
name	字符串	状态视图类型名	见 A.2.3.4 中对应状态视图类型代码的下划线字符前的部分
version	字符串	状态视图类型版本	见 A.2.3.4 中对应状态视图类型代码的下划线字符后的部分

A.3.4.3.2　通用

A.3.4.3.2.1　设备系统信息

本视图用于 SDMI::Asset::AssetAgent::queryView 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ sys－info_1.00.dtd －－>
<!ENTITY % ViewData SYSTEM "ViewData.dtd">
%ViewData;
<!ELEMENT xml (serial－num, hardware－version, software－version, manufacturer, current－time)>
<!ELEMENT serial－num (#PCDATA)>
<!ELEMENT hardware－version (#PCDATA)>
<!ELEMENT software－version (#PCDATA)>
<!ELEMENT manufacturer (#PCDATA)>
<!ELEMENT current－time (#PCDATA)>
```

设备系统信息视图参数说明见表 A.35。

表 A.35　设备系统信息视图参数说明

参数名	允许取值	说明
serial－num	字符串	设备序列号
hardware－version	字符串	硬件版本号
software－version	字符串	软件版本号
manufacturer	字符串	厂商名称
current－time	字符串	设备当前时间

A.3.4.3.2.2　网络状态信息

本视图用于 SDMI::Asset::AssetAgent::queryView 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ net－info_1.00.dtd －－>
<!ENTITY % ViewData SYSTEM "ViewData.dtd">
%ViewData;
<!ELEMENT xml (Interfaces?, RouteTable?)>
<!ENTITY % attvals.state "(connected|disconnected)">
<!ELEMENT Interface (RX?, TX?)>
<!ATTLIST Interface
    name CDATA #REQUIRED
    state %attvals.state; #REQUIRED
    mac CDATA #REQUIRED
    ip CDATA #REQUIRED
    mask CDATA #REQUIRED
    mtu CDATA #REQUIRED
>
<!ELEMENT Interfaces (Interface＋)>
<!ELEMENT RX (bytes, packets, errors, dropped, overruns, frame)>
<!ELEMENT TX (bytes, packets, errors, dropped, overruns, carrier, collisions, txqueuelent)>
```

```
<!ELEMENT bytes (#PCDATA)>
<!ELEMENT carrier (#PCDATA)>
<!ELEMENT collisions (#PCDATA)>
<!ELEMENT dropped (#PCDATA)>
<!ELEMENT errors (#PCDATA)>
<!ELEMENT frame (#PCDATA)>
<!ELEMENT overruns (#PCDATA)>
<!ELEMENT packets (#PCDATA)>
<!ELEMENT txqueuelent (#PCDATA)>
<!ELEMENT RouteTable (Route+)>
<!ELEMENT Route EMPTY>
<!ATTLIST Route
    dest CDATA #REQUIRED
    mask CDATA #REQUIRED
    gateway CDATA #REQUIRED
    flags CDATA #REQUIRED
    metric CDATA #REQUIRED
    interface CDATA #REQUIRED
>
```

网络状态信息视图参数说明见表 A.36。

表 A.36 网络状态信息视图参数说明

参数名	允许取值	说明
name	字符串	接口名称
state	connected/disconnected	连接状态
mac	MAC 地址	接口 mac 地址
ip	IP 地址	接口 ip 地址
mask	掩码	接口 ip 地址掩码
mtu	数字	接口最大传输单元
dest	IP 地址	路由目的 ip 地址
mask	掩码	路由目的 ip 地址掩码
gateway	IP 地址	网关 ip 地址
flags	字符串	路由标记
metric	数字	路由跃点
interface	字符串	路由所经过的接口名称

A.3.4.3.2.3 连接状态信息

本视图用于 SDMI::Asset::AssetAgent::queryView 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ conn－track_1.00.dtd －－>
<!ENTITY % ViewData SYSTEM "ViewData.dtd">
%ViewData;
```

```
<!ELEMENT xml (Connections)>
<!ELEMENT Connections (Connection*)>
<!ELEMENT Connection EMPTY>
<!ATTLIST Connection
    protocol CDATA #REQUIRED
    source－ip CDATA #REQUIRED
    dest－ip CDATA #REQUIRED
    source－port CDATA #IMPLIED
    dest－port CDATA #IMPLIED
    duration CDATA #REQUIRED
    state CDATA #REQUIRED
>
```

连接状态信息视图参数说明见表 A.37。

表 A.37　连接状态信息视图参数说明

参数名	允许取值	说明
protocol	tcp/udp/icmp	
source－ip	IP 地址	
dest－ip	IP 地址	
source－port	数字，0～65535	端口，
dest－port	数字，0～65535	端口，
duration	数字	持续时间，单位：秒
state	字符串	状态检测的状态

A.3.4.3.2.4　系统健康指数

本视图用于 SDMI::Asset::AssetAgent::queryView 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ health－index_1.00.dtd －－>
<!ENTITY % ViewData SYSTEM "ViewData.dtd">
%ViewData;
<!ELEMENT xml (board＋ | (cpu－usage, mem－usage, disk－usage))>
<!ELEMENT board (cpu－usage, mem－usage, (disk－usage | (sysdisk－usage, logdisk－usage)))>
<!ATTLIST board
    name CDATA #REQUIRED
    state (normal | abnormal) #REQUIRED
>
<!ELEMENT cpu－usage (#PCDATA)>
<!ELEMENT mem－usage (#PCDATA)>
<!ELEMENT disk－usage (#PCDATA)>
<!ELEMENT sysdisk－usage (#PCDATA)>
<!ELEMENT logdisk－usage (#PCDATA)>
```

系统健康指数视图参数说明见表 A.38。

表 A. 38　系统健康指数视图参数说明

参数名	允许取值	说明
cpu－usage	数字，0～100	CPU 当前使用率
mem－usage	使用量/总量	内存使用率，单位：KB
disk－usage	使用量/总量	硬盘空间使用率，单位：MB
name	字符串	用于标识隔离设备的单元
state	字符串	用于标识隔离设备单元的工作状态
sysdisk－usage	使用量/总量	系统盘空间使用率，单位：MB
logdisk－usage	使用量/总量	日志盘空间使用率，单位：MB

A. 3. 4. 3. 2. 5　代理接口信息

本视图用于 SDMI: : Asset: : AssetAgent: : queryView 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ agent－info_1.00.dtd －－>
<!ENTITY % ViewData SYSTEM "ViewData.dtd">
%ViewData;
<!ELEMENT xml (version, buildtime)>
<!ELEMENT version EMPTY>
<!ATTLIST version
    major CDATA #REQUIRED
    minor CDATA #REQUIRED
    build CDATA #REQUIRED
>
<!ELEMENT buildtime (#PCDATA)>
<!ELEMENT runtime EMPTY>
<!ATTLIST runtime
    type (device | software) #REQUIRED
    mode (single－thread | multi－thread | multi－process) CDATA #IMPLIED
    modulename CDATA #IMPLIED
>
```

代理接口信息视图参数说明见表 A.39。

表 A. 39　代理接口信息视图参数说明

参数名	允许取值	说明
major	数字	大版本号。此数值不同的管理代理彼此在接口上不能兼容。
minor	数字	小版本号。此数值不同但大版本号相同的管理代理可以向下兼容。
build	数字	安全设备厂商自用版本号。
buildtime	IDMEF 时间戳	管理代理的创建时间。
type	device/software	管理代理类型。
mode	single－thread/multi－thread/multi－process	管理代理的并发模型，可选参数。
modulename		模块名称，可选参数。

A.3.4.3.2.6 主机列表信息

本视图用于 SDMI::Asset::AssetAgent::queryView 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ host－list_1.00.dtd －－>
<!ENTITY % ViewData SYSTEM "ViewData.dtd">
%ViewData;
<!ELEMENT xml (hosts)>
<!ELEMENT hosts (host*)>
<!ATTLIST hosts
    count CDATA #REQUIRED
>
<!ELEMENT host (group?, policyarray?, loginuser?, category?, use?, location?, department?, pepsync?)>
<!ATTLIST host
    ipaddr CDATA #REQUIRED
    onlinestatus (受控 | 心跳超时 | 未部署 | 未知) #IMPLIED
>
<!ELEMENT group (#PCDATA)>
<!ELEMENT policyarray (#PCDATA)>
<!ELEMENT loginuser (#PCDATA)>
<!ELEMENT category (#PCDATA)>
<!ELEMENT use (#PCDATA)>
<!ELEMENT location (#PCDATA)>
<!ELEMENT department (#PCDATA)>
<!ELEMENT pepsync (result*)>
<!ATTLIST pepsync
    count CDATA #REQUIRED
    lastsyncedtime CDATA #REQUIRED
    error (successful | failed | never) #REQUIRED
>
<!ELEMENT result EMPTY>
<!ATTLIST result
    type CDATA #REQUIRED
    error CDATA #REQUIRED
>
```

A.3.4.3.3 防火墙/IP 访问控制规则

本视图用于 SDMI::Asset::AssetAgent::queryView 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ IpAcl－View_1.00.dtd －－>
<!ENTITY % ViewData SYSTEM "ViewData.dtd">
%ViewData;
<!ELEMENT xml (IpAcl)>
<!ENTITY % attvals.bool "(yes|no)">
```

```
<!ELEMENT Action (#PCDATA)>
<!ELEMENT Interface (#PCDATA)>
<!ELEMENT IpAcl (IpAclRule*)>
<!ELEMENT IpAclRule (Source, Target, Protocol*, Action)>
<!ATTLIST IpAclRule
    log %attvals.bool; #REQUIRED
    keep－state %attvals.bool; "yes"
>
<!ELEMENT Options (type, code)>
<!ELEMENT Protocol (sport?, dport?, Options*)>
<!ATTLIST Protocol
    name CDATA #REQUIRED
    code CDATA #REQUIRED
>
<!ELEMENT Source (address, Interface)>
<!ELEMENT Target (address, Interface)>
<!ELEMENT address (#PCDATA)>
<!ATTLIST address
    type CDATA #REQUIRED
>
<!ELEMENT code (#PCDATA)>
<!ELEMENT dport (#PCDATA)>
<!ELEMENT sport (#PCDATA)>
<!ELEMENT type (#PCDATA)>
```

IP 访问控制规则视图参数说明见表 A.40。

表 A. 40　IP 访问控制规则视图参数说明

参数名	允许取值	说明
IpAclRule 标签中的 log	yes/no	是否记录日志
IpAclRule 标签中的 keep－state	yes/no	是否保存连接
address 标签中的 type	any/addr/addr/bits/addr:mask/domain /addrGroup/!addr/addrRange	
address 标签中的 ip	根据 type 的类型取对应格式的 ip 地址，说明中标明了类型和 ip 地址的对应关系	“any(任意)” /“x.x.x.x(地址)” /“addr/bits(x.x.x.x/x)” /“addr:mask (x.x.x.x:x.x.x.x)” /www.sina.com(域名) /“x.x.x.x,x.x.x.x, addr/bits(x.x.x.x/x), addr:mask (x.x.x.x:x.x.x.x)(地址组)” /“! addr:mask (非地址)” /“ x.x.x.x－x.x.x.x(地址范围)”
Interface	字符串	接口名称
Action	deny/accept	包过滤动作
type	数字	当协议是 ICMP 的时候，填写 ICMP 的类型
code	数字	当协议是 ICMP 的时候，填写 ICMP 的类型对应的代码

A.3.4.3.4　入侵检测/引擎信息

本视图用于 SDMI::Asset::AssetAgent::queryView 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ idsengin－info_1.00.dtd －－>
<!ENTITY % ViewData SYSTEM "ViewData.dtd">
%ViewData;
<!ELEMENT xml (state, rule－template, rule－num)>
<!ELEMENT state (#PCDATA)>
<!ELEMENT rule－template (#PCDATA)>
<!ELEMENT rule－num (#PCDATA)>
```

入侵检测引擎信息视图参数说明见表 A.41。

表 A.41　入侵检测引擎信息视图参数说明

参数名	允许取值	说明
state	字符串	入侵检测引擎的工作状态
rule－template	字符串	规则模板名称
rule－num	数字	当前规则数

A.3.4.3.5　防病毒/检测引擎信息

本视图用于 SDMI::Asset::AssetAgent::queryView 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ avengin－info_1.00.dtd －－>
<!ENTITY % ViewData SYSTEM "ViewData.dtd">
%ViewData;
<!ELEMENT xml (name, version, virus－db, state)>
<!ELEMENT name (#PCDATA)>
<!ELEMENT version (#PCDATA)>
<!ELEMENT virus－db (#PCDATA)>
<!ELEMENT state (#PCDATA)>
```

病毒检测引擎信息视图参数说明见表 A.42。

表 A.42　病毒检测引擎信息视图参数说明

参数名	允许取值	说明
name	字符串	软件名称
version	字符串	引擎版本
virus－db	字符串	病毒库版本
state	字符串	引擎工作状态

A.3.4.3.6　隔离设备

A.3.4.3.6.1　注册信息

本视图用于 SDMI::Asset::AssetAgent::queryView 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ reg－info_view_1.00.dtd －－>
<!ENTITY % ViewData SYSTEM "ViewData.dtd">
```

%ViewData;
<!ELEMENT xml (reg)>
<!ELEMENT reg (vendor, gapid, section, admin, location, gapip, address)>
<!ELEMENT vendor (#PCDATA)>
<!ELEMENT gapid (#PCDATA)>
<!ELEMENT section (#PCDATA)>
<!ELEMENT admin (#PCDATA)>
<!ELEMENT location (#PCDATA)>
<!ELEMENT gapip (#PCDATA)>
<!ELEMENT address (#PCDATA)>
注册信息视图参数说明见表 A.43。

表 A.43　注册信息视图参数说明

参数名	允许取值	说明
vendor	字符串	提供商标识
gapid	字符串	铭牌标识
section	字符串	使用单位
admin	字符串	责任人
location	字符串	地理位置
gapip	字符串	管理 IP 地址
address	字符串	联系方式

A.3.4.3.6.2　隔离策略

本视图用于 SDMI::Asset::AssetAgent::queryView 方法，见 A.1.2.6。
<?xml version="1.0" encoding="UTF－8"?>
<!－－ Isolation－policy_view_1.00.dtd －－>
<!ENTITY % ViewData SYSTEM "ViewData.dtd">
%ViewData;
<!ELEMENT xml (rules?, objects?)>
<!ELEMENT rules (rule＋)>
<!ELEMENT rule (enable, name, service, source, destination, sn?, application?, keyword?, time?, action, log, direction?, reflection)>
<!ELEMENT objects (object＋)>
<!ELEMENT object (type, name, inout?, ip?,protocol?, property?, basesetnum?, basename1?, basevalue1?, advancesetnum?, advancename1?, advancevalue1?, advancename2?, advancevalue1?, advancevalue2?, advancename3?, advancevalue3?, advancename4?, advancevalue4?, advancename5?, advancevalue5?, advancename6?, advancevalue6?, advancename7?, advancevalue7?, key?, note?, group?, inout?, ip?)>
<!ELEMENT action (#PCDATA)>
<!ELEMENT advancename1 (#PCDATA)>
<!ELEMENT advancename2 (#PCDATA)>
<!ELEMENT advancename3 (#PCDATA)>
<!ELEMENT advancename4 (#PCDATA)>

<!ELEMENT advancename5 (#PCDATA)>
<!ELEMENT advancename6 (#PCDATA)>
<!ELEMENT advancename7 (#PCDATA)>
<!ELEMENT advancesetnum (#PCDATA)>
<!ELEMENT advancevalue1 (#PCDATA)>
<!ELEMENT advancevalue2 (#PCDATA)>
<!ELEMENT advancevalue3 (#PCDATA)>
<!ELEMENT advancevalue4 (#PCDATA)>
<!ELEMENT advancevalue5 (#PCDATA)>
<!ELEMENT advancevalue6 (#PCDATA)>
<!ELEMENT advancevalue7 (#PCDATA)>
<!ELEMENT application (#PCDATA)>
<!ELEMENT basename1 (#PCDATA)>
<!ELEMENT basesetnum (#PCDATA)>
<!ELEMENT basevalue1 (#PCDATA)>
<!ELEMENT destination (#PCDATA)>
<!ELEMENT direction (#PCDATA)>
<!ELEMENT enable (#PCDATA)>
<!ELEMENT group (#PCDATA)>
<!ELEMENT inout (#PCDATA)>
<!ELEMENT ip (#PCDATA)>
<!ELEMENT key (#PCDATA)>
<!ELEMENT keyword (#PCDATA)>
<!ELEMENT log (#PCDATA)>
<!ELEMENT name (#PCDATA)>
<!ELEMENT note (#PCDATA)>
<!ELEMENT property (#PCDATA)>
<!ELEMENT protocol (#PCDATA)>
<!ELEMENT reflection (#PCDATA)>
<!ELEMENT service (#PCDATA)>
<!ELEMENT sn (#PCDATA)>
<!ELEMENT source (#PCDATA)>
<!ELEMENT time (#PCDATA)>
<!ELEMENT type (#PCDATA)>

其中，object 标签内的内容见表 A.44，rule 标签内的内容见表 A.45。

表 A.44　对象节点参数

对象类型	标签名	允许取值	说明
地址对象	type	address	地址对象类型
	name	自定义字符串	地址对象名称
	inout	内网对象 外网对象 不区别内外网对象	内网或外网

表 A.44(续)

对象类型	标签名	允许取值	说明
地址对象	ip	自定义字符串 [ip1]/[mask1]，[ip2]/[mask2]……	地址组或地址范围
	note	描述字符串	备注描述
	group	自定义字符串，可用来表示对象组中的对象名列表	作为地址组对象的扩展
服务对象	type	service	服务对象类型
	name	自定义字符串，已有服务应按照以下列出名称命名 短报文 文电 实时报文 名录服务 ospf/bgp/rip/ping/traceroute	服务对象名称
	protocol	自定义字符串，表示 ip 层协议域相关内容	协议类型
	property	自定义字符串，属性描述	端口列表、协议号、跳数等服务属性
长报文应用层对象	type	application	军用应用层对象类型
	name	自定义字符串	
	protocol	长报文应用对象	
	basesetnum	1	
	basename1	版本号	
	basevalue1	字符串	
	advancesetnum	1	
	advancename1		
	advancevalue1		
	note	描述字符串	备注描述
	group	自定义字符串，可用来表示对象组中的对象名列表	
实时报文应用层对象	type	application	
	name	自定义字符串	
	protocol	“实时报文应用对象”	
	basesetnum	1	基本控制属性总数
	basename1	“发送方接收方标识”	
	basevalue1	属性描述字符串	实体标识字符串
	advancesetnum	2	
	advancename1	“数据报文类型”	数据报文项使能
	advancevalue1	预警探测，指控……中的一个或几个，“，”分割	数据控制类型
	advancename2	“控制报文类型”	控制报文项使能
	advancevalue2	参数设置报文，接入申请报文……中的一个或几个，“，”分割	数据控制类型
	note	描述字符串	备注描述
	group	自定义字符串，可用来表示对象组中的对象名列表	

表 A. 44(续)

对象类型	标签名	允许取值	说明
实时报文应用层对象	type	application	
	name	自定义字符串	
	protocol	“短报文应用对象”	
	basesetnum	1	基本控制属性总数
	basename1	“端口标识”	
	basevalue1	源端口标识 目的端口标识	端口标识属性定义
	advancesetnum	7	
	advancename1	“作战单元编号”	
	advancevalue1	字符串	
	advancename2	“格式类型”	
	advancevalue2	战术数据，战术数据扩展……中的一个或几个，用“,”分割	
	advancename3	“密级”	
	advancevalue3	核心机密，绝密……中的一个或几个，用“,”分割	
	advancename4	“优先级”	
	advancevalue4	限时，特急……中的一个或几个，用“,”分割	
	advancename5	“功能域”	
	advancevalue5	通用通信，火力支援……中的一个或几个，用“,”分割	
	advancename6	“状态域”	
	advancevalue6	演习、测试……中的一个或几个，用“,”分割	
	advancename7	“关键字”	
	advancevalue7	关键字字符串	
	note	描述字符串	备注描述
	group	自定义字符串，可用来表示对象组中的对象名列表	
时统	type	application	时统协议对象描述
	name	自定义字符串	
	protocol	“时统报文应用对象”	
	basesetnum	1	基本控制属性总数
	basename1	“端口标识”	
	basevalue1	源端口标识 目的端口标识	端口标识属性定义
	note	描述字符串	备注描述
	group	自定义字符串，可用来表示对象组中的对象名列表	
61A/62A	type	application	海军 6162 协议对象描述
	name	自定义字符串	
	protocol	“海军 6162 报文应用对象”	
	basesetnum	1	基本控制属性总数

表 A.44(续)

对象类型	标签名	允许取值	说明
61A/62A	basename1	“发送方接收方标识”	
	basevalue1	字符串 [源][系统标识]-[主机标识]-[实体识][目的][系统标识]-[主机标识]-[实体标识]	实体标识字符串
	advanceset	enable/disable	
	advancesetnum	2	
	advancename1	“数据报文类型”	数据报文项使能
	advancevalue1	预警探测，指控……	数据控制类型
	advancename2	“控制报文类型”	控制报文项使能
	advancevalue2	参数设置报文，接入申请报文……	数据控制类型
	note	描述字符串	备注描述
	group	自定义字符串，可用来表示对象组中的对象名列表	
x 协议	type	application	X 协议对象描述规范
	name	自定义字符串	
	protocol	扩展应用对象 xx 报文应用对象自定义字符串(服务对象名)	
	basesetnum	n 基本控制属性的个数	基本控制属性总数
	basename1	属性 1 名称	基本控制属性 1 使能
	basevalue1	描述字符串	基本控制属性 1
	basename2	属性 2 名称	基本控制属性 2 使能
	basevalue2	描述字符串	基本控制属性 2
	…		迭代至 basesetnum 为止
	basenamen	属性 n 名称	基本控制属性 n 使能
	basevaluen	描述字符串	基本控制属性 n
	advancesetnum	m 高级控制属性的个数	高级控制属性总数
	advancename1	属性名称	高级控制属性 1 使能
	advancevalue1	描述字符串	高级控制属性 1
	advancename2	属性名称	高级控制属性 2 使能
	advancevalue2	描述字符串	高级控制属性 2
	…		迭代至 advancesetnum 为止
	advancenamem	属性 m 名称	高级控制属性 n 使能
	advancevaluem	描述字符串	高级控制属性 M
	note	描述字符串	备注描述
	group	自定义字符串，可用来表示对象组中的对象名列表	
时间对象	type	time	时间对象类型
	name	自定义字符串	
	property	字符串	

表 A.44(续)

对象类型	标签名	允许取值	说明
时间对象	note	描述字符串	备注描述
	group	自定义字符串，可用来表示对象组中的对象名列表	
关键字过滤对象	type	keyword	表示为关键字过滤对象
	name	自定义字符串	
	key	字符串，关键字列表	

表 A.45 规则节点参数

标签名	允许取值	说明
name	自定义	说明
service	在预定义服务中选择	
source	在已定义的地址对象中选择	
destination	在已定义的地址对象中选择	
application	在已定义的应用层对象中选择	没有写为空串
action	自定义字符串“允许/禁止”	
time	在已定义的时间对象中选择	
keyword	关键字对象	没有写为空串
log	on/off	记录/不记录
enable	on/off	开/关
direction	自定义字符串	没有则填空串(方向)
reflection	自定义字符串	没有则填空串(反射选项)

A.3.4.3.7 数据库审计

A.3.4.3.7.1 审计节点审计管理

本视图用于 SDMI::Asset::AssetAgent::queryView 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- AUDIT_SERVER_AUDIT_VIEW_1.00.dtd -->
<!ENTITY % ViewData SYSTEM "ViewData.dtd">
%ViewData;
<!ELEMENT xml (SHOW_AUDIT_CONF, SHOW_ADUT_EVENT)>
<!ELEMENT INFO (#PCDATA)>
<!ATTLIST INFO
    CONF_ID CDATA #IMPLIED
    AU_USER_ID CDATA #IMPLIED
    INSTANCE CDATA #IMPLIED
    SCHEMA CDATA #IMPLIED
    OBJECT CDATA #IMPLIED
    EVENT CDATA #REQUIRED
    RESULT CDATA #REQUIRED
```

```
    SERVICE CDATA #IMPLIED
    USER CDATA #IMPLIED
    HOST CDATA #IMPLIED
    TASKID CDATA #IMPLIED
    DATE CDATA #IMPLIED
    DES CDATA #IMPLIED
>
<!ELEMENT SHOW_ADUT_EVENT (INFO*)>
<!ELEMENT SHOW_AUDIT_CONF (INFO*)>
```

审计节点审计管理视图参数说明见表 A.46。

表 A.46　审计节点审计管理视图参数说明

参数名	允许取值	说明
SHOW_AUDIT_CONF 标签中的 CONF_ID	字符串	审计规则 ID
SHOW_AUDIT_CONF 标签中的 AU_USER_ID	字符串	审计用户 ID
SHOW_AUDIT_CONF 标签中的 INSTANCE	字符串	Oracle 实例名
SHOW_AUDIT_CONF 标签中的 SCHEMA	字符串	模式名
SHOW_AUDIT_CONF 标签中的 OBJECT	字符串	对象名
SHOW_AUDIT_CONF 标签中的 EVENT	字符串	事件类型
SHOW_AUDIT_CONF 标签中的 RESULT	字符串	结果类型
SHOW_ADUT_EVENT 标签中的 SERVICE	字符串	实例名
SHOW_ADUT_EVENT 标签中的 USER	字符串	用户名
SHOW_ADUT_EVENT 标签中的 HOST	字符串	主机地址
SHOW_ADUT_EVENT 标签中的 TASKID	字符串	任务号
SHOW_ADUT_EVENT 标签中的 DATE	字符串	日期
SHOW_ADUT_EVENT 标签中的 EVENT	字符串	语句
SHOW_ADUT_EVENT 标签中的 RESULT	字符串	结果
SHOW_ADUT_EVENT 标签中的 DES	字符串	描述

A.3.4.3.7.2　审计节点配置管理

本视图用于 SDMI::Asset::AssetAgent::queryView 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- AUDIT_SERVER_CONF_VIEW_1.00.dtd -->
<!ENTITY % ViewData SYSTEM "ViewData.dtd">
%ViewData;
<!ELEMENT xml (SHOW_ALL_SERVER, SHOW_SPEC_SERVER)>
<!ELEMENT INFO EMPTY>
<!ATTLIST INFO
    IP CDATA #REQUIRED
    STATUS CDATA #IMPLIED
    AUDIT_STATUS CDATA #IMPLIED
    DES CDATA #IMPLIED
```

>
<!ELEMENT SHOW_ALL_SERVER (INFO*)>
<!ELEMENT SHOW_SPEC_SERVER (INFO*)>
审计节点配置管理视图参数说明见表 A.47。

表 A. 47　审计节点配置管理视图参数说明

参数名	允许取值	说明
SHOW_ALL_SERVER 标签中的 IP	字符串	节点地址
SHOW_ALL_SERVER 标签中的 STATUS	字符串	节点状态
SHOW_SPEC_SERVER 标签中的 IP	字符串	节点地址
SHOW_SPEC_SERVER 标签中的 AUDIT_STATUS	字符串	审计开关
SHOW_SPEC_SERVER 标签中的 DES	字符串	提示信息

A. 3. 4. 3. 7. 3　Oracle 信息

本视图用于 SDMI: : Asset: : AssetAgent: : queryView 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ ORACLE_INFO_VIEW_1.00.dtd －－>
<!ENTITY % ViewData SYSTEM "ViewData.dtd">
%ViewData;
<!ELEMENT xml (SHOW_INSTANCE*)>
<!ELEMENT COLUMN (#PCDATA)>
<!ATTLIST COLUMN
    NAME CDATA #REQUIRED
>
<!ELEMENT NAME (#PCDATA)>
<!ATTLIST NAME
    VALUE CDATA #REQUIRED
>
<!ELEMENT SCHEMA (TABLE*)>
<!ATTLIST SCHEMA
    NAME CDATA #REQUIRED
>
<!ELEMENT SHOW_ALL_ORACLE_OBJ (SCHEMA*)>
<!ELEMENT SHOW_ALL_ORACLE_SUB (NAME*)>
<!ELEMENT SHOW_INSTANCE (SHOW_ALL_ORACLE_OBJ, SHOW_ALL_ORACLE_SUB)>
<!ATTLIST SHOW_INSTANCE
    NAME CDATA #REQUIRED
>
<!ELEMENT TABLE (COLUMN*)>
<!ATTLIST TABLE
    NAME CDATA #REQUIRED
>
```

Oracle 信息视图参数说明见表 A.48。

表 A.48 Oracle 信息视图参数说明

参数名	允许取值	说明
SHOW_INSTANCE 标签中的 NAME	字符串	数据库实例名称
SCHEMA 标签中的 NAME	字符串	数据库名称
TABLE 标签中的 NAME	字符串	数据库表明
COLUMN 标签中的 NAME	字符串	数据库列名
NAME 标签中的 VALUE	字符串	数据库用户名称

A.3.4.3.7.4 访问控制节点配置管理

本视图用于 SDMI::Asset::AssetAgent::queryView 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF−8"?>
<!−− SEC_SERVER_CONF_VIEW_1.00.dtd −−>
<!ENTITY % ViewData SYSTEM "ViewData.dtd">
%ViewData;
<!ELEMENT xml (SHOW_ALL_SERVER)>
<!ELEMENT INFO EMPTY>
<!ATTLIST INFO
    IP CDATA #REQUIRED
    STATUS CDATA #REQUIRED
>
```

访问控制节点配置管理视图参数说明见表 A.49。

表 A.49 访问控制节点配置管理视图参数说明

参数名	允许取值	说明
INFO 标签中的 IP	字符串	访问控制节点的 IP 地址
INFO 标签中的 STATUS	字符串	节点状态

A.3.4.3.7.5 访问控制节点安全管理

本视图用于 SDMI::Asset::AssetAgent::queryView 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF−8"?>
<!−− SEC_SERVER_SEC_VIEW.dtd −−>
<!ENTITY % ViewData SYSTEM "ViewData.dtd">
%ViewData;
<!ELEMENT xml (SHOW_ROLES, SHOW_ROLES_PRIV*)>
<!ELEMENT COLUMN_PRIV (string*)>
<!ATTLIST COLUMN_PRIV
    NAME CDATA #REQUIRED
    VALUE CDATA #REQUIRED
>
<!ELEMENT CONSTRAIN EMPTY>
<!ATTLIST CONSTRAIN
    VALUE CDATA #REQUIRED
>
```

```
<!ELEMENT GLOBAL_PRIV EMPTY>
<!ATTLIST GLOBAL_PRIV
    VALUE CDATA #REQUIRED
>
<!ELEMENT SHOW_ROLE (USER*)>
<!ATTLIST SHOW_ROLE
    NAME CDATA #REQUIRED
>
<!ELEMENT SHOW_ROLES (SHOW_ROLE*)>
<!ELEMENT SHOW_ROLES_PRIV (GLOBAL_PRIV, TABLE_PRIV*)>
<!ATTLIST SHOW_ROLES_PRIV
    NAME CDATA #REQUIRED
>
<!ELEMENT TABLE_PRIV (COLUMN_PRIV*, CONSTRAIN)>
<!ATTLIST TABLE_PRIV
    NAME CDATA #REQUIRED
    VALUE CDATA #REQUIRED
>
<!ELEMENT USER EMPTY>
<!ATTLIST USER
    NAME CDATA #REQUIRED
>
```

访问控制节点安全管理视图参数说明见表 A.50。

表 A. 50　访问控制节点安全管理视图参数说明

参数名	允许取值	说明
SHOW_ROLE 标签中的 NAME	字符串	角色名
USER 标签中的 NAME	字符串	角色名
SHOW_ROLES_PRIV 标签中的 NAME	字符串	角色名
GLOBAL_PRIV 标签中的 VALUE	字符串	全局权限
TABLE_PRIV 标签中的 NAME	字符串	表名
TABLE_PRIV 标签中的 VALUE	字符串	表级权限
COLUMN_PRIV 标签中的 VALUE	字符串	列级权限
CONSTRAIN 标签中的 VALUE	字符串	行级约束

A. 3. 4. 3. 7. 6　系统信息管理

本视图用于 SDMI: : Asset: : AssetAgent: : queryView 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ SYS_VIEW.dtd －－>
<!ENTITY % ViewData SYSTEM "ViewData.dtd">
%ViewData;
<!ELEMENT xml (SHOW_INSTANCE*)>
<!ELEMENT AU_USER (#PCDATA)>
```

```
<!ATTLIST AU_USER
    NAME CDATA #REQUIRED
    ID CDATA #REQUIRED
>
<!ELEMENT SHOW_AU_USER (AU_USER*)>
<!ELEMENT SHOW_INSTANCE (SHOW_AU_USER)>
<!ATTLIST SHOW_INSTANCE
    NAME CDATA #REQUIRED
>
```

系统信息管理视图参数说明见表 A.51。

表 A.51　系统信息管理视图参数说明

参数名	允许取值	说明
SHOW_INSTANCE 标签中的 NAME	字符串	数据库实例名
AU_USER 标签中的 NAME	字符串	审计用户角色名
AU_USER 标签中的 ID	字符串	审计用户 ID

A.3.4.3.8　漏洞扫描

A.3.4.3.8.1　漏洞扫描引擎

本视图用于 SDMI::Asset::AssetAgent::queryView 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ Vulengin－info_1.00.dtd －－>
<!ENTITY % ViewData SYSTEM "ViewData.dtd">
%ViewData;
<!ELEMENT xml (name, version, vul－db, vul－num, scan_num)>
<!ELEMENT name (#PCDATA)>
<!ELEMENT version (#PCDATA)>
<!ELEMENT vul－db (#PCDATA)>
<!ELEMENT vul－num (#PCDATA)>
<!ELEMENT scan_num (#PCDATA)>
```

漏洞扫描引擎视图参数说明见表 A.52。

表 A.52　漏洞扫描引擎视图参数说明

参数名	允许取值	说明
name	字符串	软件名称
version	字符串	引擎版本
vul－db	字符串	漏洞库版本
vul－num	数字	漏洞数
scan_num	数字	当前正在扫描任务数量

A.3.4.3.8.2　漏洞扫描任务列表

本视图用于 SDMI::Asset::AssetAgent::queryView 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ VulnerabilityList_1.00.dtd －－>
```

<!ENTITY % ViewData SYSTEM "ViewData.dtd">
%ViewData;
<!ELEMENT xml (scan_task*)>
<!ELEMENT scan_task (scan_name, scan_state, scan_progress)>
<!ELEMENT scan_name (#PCDATA)>
<!ELEMENT scan_state (#PCDATA)>
<!ELEMENT scan_progress (#PCDATA)>
漏洞扫描任务视图参数说明见表 A.53。

表 A.53 漏洞扫描任务视图参数说明

参数名	允许取值	说明
scan_name	字符串	扫描任务名称
scan_state	wait/scan/end	引擎版本
scan_progress	数字，0～100	正在扫描的任务的进度

A.3.4.3.8.3 漏洞扫描结果

本视图用于 SDMI::Asset::AssetAgent::queryView 方法，见 A.1.2.6。

<?xml version="1.0" encoding="UTF-8"?>
<!-- VulnerabilityResult_1.00.dtd -->
<!ENTITY % ViewData SYSTEM "ViewData.dtd">
%ViewData;
<!ENTITY % Address SYSTEM "Address.dtd">
%Address;
<!ELEMENT xml (scan_info, scan_result)>
<!ELEMENT scan_info (state, TimeSpan)>
<!ELEMENT state (#PCDATA)>
<!ELEMENT TimeSpan (start-time, end-time)>
<!ATTLIST TimeSpan
type CDATA #FIXED "fromto"
>
<!ELEMENT start-time (year, month, day-of-month, hour, minutes, second)>
<!ELEMENT year (#PCDATA)>
<!ELEMENT month (#PCDATA)>
<!ELEMENT day-of-month (#PCDATA)>
<!ELEMENT hour (#PCDATA)>
<!ELEMENT minutes (#PCDATA)>
<!ELEMENT second (#PCDATA)>
<!ELEMENT end-time (year, month, day-of-month, hour, minutes, second)>
<!ELEMENT scan_result (host_info, flaw_info, port_info, share_info, host_user_info, service_info, service_user_info)>
<!ELEMENT host_info (host_id, Address, TimeSpan, host_name, workgroup, os, mac, online_flag)>
<!ELEMENT host_id (#PCDATA)>
<!ELEMENT host_name (#PCDATA)>

<!ELEMENT workgroup (#PCDATA)>
<!ELEMENT os (#PCDATA)>
<!ELEMENT mac (#PCDATA)>
<!ELEMENT online_flag (#PCDATA)>
<!ELEMENT flaw_info (host_id, vul_id, vul_name, flaw_scan_info, flaw_port)>
<!ELEMENT vul_id (#PCDATA)>
<!ELEMENT vul_name (#PCDATA)>
<!ELEMENT flaw_scan_info (#PCDATA)>
<!ELEMENT flaw_port (#PCDATA)>
<!ELEMENT port_info (host_id, port, protocol, service_name, service_version)>
<!ELEMENT port (#PCDATA)>
<!ELEMENT protocol (#PCDATA)>
<!ELEMENT service_name (#PCDATA)>
<!ELEMENT service_version (#PCDATA)>
<!ELEMENT share_info (host_id, share_name, share_type, share_content)>
<!ELEMENT share_name (#PCDATA)>
<!ELEMENT share_type (#PCDATA)>
<!ELEMENT share_content (#PCDATA)>
<!ELEMENT host_user_info (host_id, user_name, password, login_time, changepassword_time, user_scripts)>
<!ELEMENT user_name (#PCDATA)>
<!ELEMENT password (#PCDATA)>
<!ELEMENT login_time (#PCDATA)>
<!ELEMENT changepassword_time (#PCDATA)>
<!ELEMENT user_scripts (#PCDATA)>
<!ELEMENT service_info (host_id, service_name, service_summary)>
<!ELEMENT service_summary (#PCDATA)>
<!ELEMENT service_user_info (host_id, service_name, user_name, password)>

A.3.4.3.8.4 漏洞信息

本视图用于 SDMI::Asset::AssetAgent::queryView 方法，见 A.1.2.6。

<?xml version="1.0" encoding="UTF－8"?>
<!－－ VulInfo_1.00.dtd －－>
<!ENTITY % ViewData SYSTEM "ViewData.dtd">
%ViewData;
<!ELEMENT xml (VulInfo*)>
<!ELEMENT VulInfo (vul_id, cve_no, bugtraq_id, vul_name, risk_level, descript, solution)>
<!ELEMENT vul_id (#PCDATA)>
<!ELEMENT cve_no (#PCDATA)>
<!ELEMENT bugtraq_id (#PCDATA)>
<!ELEMENT vul_name (#PCDATA)>
<!ELEMENT risk_level (#PCDATA)>
<!ELEMENT descript (#PCDATA)>
<!ELEMENT solution (#PCDATA)>

漏洞信息视图参数说明见表 A.54。

表 A.54 漏洞信息视图参数说明

参数名	允许取值	说明
vul_id	字符串	漏洞编号
cve_no	字符串	CVE 编号
bugtraq_id	字符串	bugtraq 号
vul_name	字符串	漏洞名称
risk_level	字符串	风险级别
descript	字符串	漏洞描述
solution	字符串	解决方案

A.3.4.3.9 补丁管理

A.3.4.3.9.1 补丁安装信息

本视图用于 SDMI::Asset::AssetAgent::queryView 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Patch-Info_1.00.dtd -->
<!ENTITY % ViewData SYSTEM "ViewData.dtd">
%ViewData;
<!ELEMENT xml (PacthInfo)>
<!ELEMENT PacthInfo (Map, Install, UnInstall)>
<!ELEMENT Install (iteminstall+)>
<!ATTLIST Install
    Count CDATA #REQUIRED
>
<!ELEMENT InstallBy (#PCDATA)>
<!ELEMENT InstallCode (#PCDATA)>
<!ELEMENT InstallDate (#PCDATA)>
<!ELEMENT InstallDescription (#PCDATA)>
<!ELEMENT InstallLevel (#PCDATA)>
<!ELEMENT InstallOstype (#PCDATA)>
<!ELEMENT InstallType (#PCDATA)>
<!ELEMENT Map (type+)>
<!ELEMENT UnInstall (itemuninstall)>
<!ATTLIST UnInstall
    Count CDATA #REQUIRED
>
<!ELEMENT UninsCode (#PCDATA)>
<!ELEMENT UninsDescription (#PCDATA)>
<!ELEMENT UninsLevel (#PCDATA)>
<!ELEMENT UninsPath (#PCDATA)>
<!ELEMENT UninsType (#PCDATA)>
<!ELEMENT iteminstall (InstallCode, InstallBy, InstallDate, InstallType, InstallDescription,
```

InstallOstype?, InstallLevel?)>

<!ELEMENT itemuninstall (UninsCode, UninsPath, UninsType, UninsLevel, UninsDescription)>

<!ELEMENT type (#PCDATA)>

<!ATTLIST type

key CDATA #REQUIRED

>

补丁安装信息视图参数说明见表 A.55。

表 A. 55　补丁安装信息视图参数说明

参数名	允许取值	说明
InstallCode	字符串	已安装补丁名称
InstallBy	字符串	已安装补丁安装时的用户身份
InstallDate	字符串	已安装补丁的安装时间
InstallType	字符串	已安装补丁类型
InstallDescription	字符串	已安装补丁的漏洞描述
InstallOstype	字符串	已安装补丁的操作系统类型
UninsCode	字符串	未安装补丁名称
UninsPath	字符串	未安装补丁的文件名称
UninsType	字符串	未安装补丁类型
UninsLevel	字符串	未安装补丁级别
UninsDescription	字符串	未安装补丁的漏洞描述

A. 3. 4. 3. 9. 2　补丁库列表

本视图用于 SDMI::Asset::AssetAgent::queryView 方法，见 A.1.2.6。

<?xml version="1.0" encoding="UTF－8"?>

<!－－ Patch－List_1.00.dtd －－>

<!ENTITY % ViewData SYSTEM "ViewData.dtd">

%ViewData;

<!ELEMENT xml (PatchList)>

<!ELEMENT PatchList (Map*)>

<!ELEMENT Map (type＋)>

<!ELEMENT type (#PCDATA)>

<!ATTLIST type

key CDATA #REQUIRED

>

补丁库列表视图 type 参数说明见表 A.56。

表 A. 56　补丁库列表视图 type 参数说明

参数名	允许取值	说明
PatchCode	字符串	补丁号
PatchLevel	01/2/3/4	补丁级别
PatchDescription	字符串	补丁的漏洞描述

表 A.56(续)

参数名	允许取值	说明
PatchType	字符串	补丁类型
PatchOstype	字符串	补丁的操作系统类型
PatchLanguage	字符串	补丁语言

A.3.4.3.10 主机监控

A.3.4.3.10.1 主机组列表信息

本视图用于 SDMI::Asset::AssetAgent::queryView 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- hw-hostgroup-list_1.00.dtd -->
<!ENTITY % ViewData SYSTEM "ViewData.dtd">
%ViewData;
<!ELEMENT xml (hostgroups)>
<!ELEMENT hostgroups (hostgroup*)>
<!ATTLIST hostgroups
    count CDATA #REQUIRED
>
<!ELEMENT hostgroup (name, policyarray, description)>
<!ATTLIST hostgroup
    onlinecount CDATA #REQUIRED
    totalcount CDATA #REQUIRED
>
<!ELEMENT name (#PCDATA)>
<!ELEMENT policyarray (#PCDATA)>
<!ELEMENT description (#PCDATA)>
```

A.3.4.3.10.2 用户组列表信息

本视图用于 SDMI::Asset::AssetAgent::queryView 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- hw-usergroup-list_1.00.dtd -->
<!ENTITY % ViewData SYSTEM "ViewData.dtd">
%ViewData;
<!ELEMENT xml (usergroups)>
<!ELEMENT usergroups (usergroup*)>
<!ATTLIST usergroups
    count CDATA #REQUIRED
>
<!ELEMENT usergroup (name, description)>
<!ATTLIST usergroup
    onlinecount CDATA #REQUIRED
    totalcount CDATA #REQUIRED
>
<!ELEMENT name (#PCDATA)>
```

```
<!ELEMENT description (#PCDATA)>
```

A. 3. 4. 3. 10. 3　用户列表信息

本视图用于 SDMI: : Asset: : AssetAgent: : queryView 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ hw－user－list_1.00.dtd －－>
<!ENTITY % ViewData SYSTEM "ViewData.dtd">
%ViewData;
<!ENTITY % attvals.yesno "( yes | no )">
<!ELEMENT xml (users)>
<!ELEMENT users (user*)>
<!ATTLIST users
    count CDATA #REQUIRED
>
<!ELEMENT user (group, name, username, tokenid, department, duty, phonenum, site)>
<!ATTLIST user
    isadmin %attvals.yesno; #REQUIRED
    isusb %attvals.yesno; #REQUIRED
    status (登录 | 注销 | 未使用 | 未知) #REQUIRED
    ipaddr CDATA #REQUIRED
>
<!ELEMENT group (#PCDATA)>
<!ELEMENT name (#PCDATA)>
<!ELEMENT username (#PCDATA)>
<!ELEMENT tokenid (#PCDATA)>
<!ELEMENT department (#PCDATA)>
<!ELEMENT duty (#PCDATA)>
<!ELEMENT phonenum (#PCDATA)>
<!ELEMENT site (#PCDATA)>
```

A. 3. 4. 3. 10. 4　服务器统计信息

本视图用于 SDMI: : Asset: : AssetAgent: : queryView 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ hw－server－stat_1.00.dtd －－>
<!ENTITY % ViewData SYSTEM "ViewData.dtd">
%ViewData;
<!ELEMENT xml (hoststat, userstat, alertstat?)>
<!ELEMENT hoststat (total, status, policy)>
<!ELEMENT total EMPTY>
<!ATTLIST total
    group CDATA #REQUIRED
    item CDATA #REQUIRED
>
<!ELEMENT status EMPTY>
<!ATTLIST status
```

```
    online CDATA #REQUIRED
    offline CDATA #REQUIRED
    unused CDATA #REQUIRED
>
<!ELEMENT policy EMPTY>
<!ATTLIST policy
    successful CDATA #REQUIRED
    failed CDATA #REQUIRED
    never CDATA #REQUIRED
>
<!ELEMENT userstat (total, status, mode)>
<!ELEMENT mode EMPTY>
<!ATTLIST mode
    bypwd CDATA #REQUIRED
    byusb CDATA #REQUIRED
>
<!ELEMENT alertstat (treatment, level)>
<!ELEMENT treatment EMPTY>
<!ATTLIST treatment
    treated CDATA #REQUIRED
    untreated CDATA #REQUIRED
>
<!ELEMENT level EMPTY>
<!ATTLIST level
    fatal CDATA #REQUIRED
    serious CDATA #REQUIRED
    common CDATA #REQUIRED
>
```

A.3.5 维护性操作

A.3.5.1 通用操作

A.3.5.1.1 封包格式

通用操作的参数封包遵循 GeneralOperation.dtd 的约束。GeneralOperation.dtd 的内容如下：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- GeneralOperation.dtd -->
<!ENTITY % CreateTime SYSTEM "CreateTime.dtd">
%CreateTime;
<!ELEMENT PolicyPack (Policy)>
<!ELEMENT Policy (CreateTime, Operation)>
<!ATTLIST Policy
    type CDATA #FIXED "Operation"
    version CDATA #FIXED "1.00"
    description CDATA #FIXED "通用操作"
    mode CDATA #FIXED "transient"
```

>

通用操作类型见表 A.57。

表 A.57　通用操作类型

代码	类别
reboot	重启设备
shutdown	关闭设备
save	保存配置
settime	设置时间
upgrade	手动升级

A.3.5.1.2　时间设定

本操作用于 SDMI::Policy::PolicyExecutor::fill 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ GO_set－time.dtd －－>
<!ENTITY % GeneralOperation SYSTEM "GeneralOperation.dtd">
%GeneralOperation;
<!ELEMENT Operation (AdditionalData)>
<!ATTLIST Operation
    type CDATA #FIXED "set－time"
>
<!ELEMENT AdditionalData (date－time)>
<!ATTLIST AdditionalData
    meaning CDATA #FIXED "date－time"
    type CDATA #FIXED "date－time">
<!ELEMENT date－time (#PCDATA)>
```

时间设定操作参数说明见表 A.58。

表 A.58　时间设定操作参数说明

参数名	允许取值	说明
date－time	填写 IDMEF 格式的时间字符串	见 A.2.1.2.2

A.3.5.1.3　关机/重启

本操作用于 SDMI::Policy::PolicyExecutor::fill 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ GO_reboot_shutdown_1.00.dtd －－>
<!ENTITY % GeneralOperation SYSTEM "GeneralOperation.dtd">
%GeneralOperation;
<!ELEMENT Operation (AdditionalData, AdditionalData)>
<!ATTLIST Operation
    type (reboot | shutdown) #REQUIRED
>
<!ELEMENT AdditionalData (integer | string)>
<!ATTLIST AdditionalData
```

```
    meaning (delay | reason) #REQUIRED
    type (integer | string) "string"
>
<!ELEMENT integer (#PCDATA)>
<!ELEMENT string (#PCDATA)>
```

关机/重启操作参数说明见表 A.59。

表 A.59 关机/重启操作参数说明

参数名	允许取值	说明
delay	数字	填写关机延迟的秒数，单位：秒
reason	字符串	填写关机重启的原因

A.3.5.1.4 手动升级

本操作用于 SDMI::Policy::PolicyExecutor::fill 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- GO_upgrade_1.00.dtd -->
<!ENTITY % GeneralOperation SYSTEM "GeneralOperation.dtd">
%GeneralOperation;
<!ELEMENT Operation (AdditionalData, (AdditionalData, AdditionalData, AdditionalData)?)>
<!ATTLIST Operation
    type CDATA #FIXED "upgrade"
>
<!ELEMENT AdditionalData (portlist | string)>
<!ATTLIST AdditionalData
    meaning (server | protocol | port | file) #REQUIRED
    type (portlist | string) "string"
>
<!ELEMENT portlist (#PCDATA)>
<!ELEMENT string (#PCDATA)>
```

手动升级操作参数说明见表 A.60。

表 A.60 手动升级操作参数说明

参数名	允许取值	说明
server	IP 地址	服务器地址
protocol	字符串	协议
portlist	数字，0～65535	服务器端口
file	字符串	文件路径

A.3.5.1.5 保存配置

本操作用于 SDMI::Policy::PolicyExecutor::fill 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- GO_save_1.00.dtd -->
<!ENTITY % GeneralOperation SYSTEM "GeneralOperation.dtd">
%GeneralOperation;
```

```
<!ELEMENT Operation (AdditionalData)>
<!ATTLIST Operation
    type CDATA #FIXED "save"
>
<!ELEMENT AdditionalData (string)>
<!ATTLIST AdditionalData
    meaning CDATA #FIXED "types"
    type (string) "string"
>
<!ELEMENT string (#PCDATA)>
```

保存配置操作参数说明见表 A.61。

表 A.61　保存配置操作参数说明

参数名	允许取值	说明
types	用逗号隔开的字符串	要保存的安全策略名称

A.3.5.2　专用操作

A.3.5.2.1　封包格式

专用操作的参数封包遵循 Operation.dtd 的约束。Operation.dtd 的内容如下：

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ Operation.dtd －－>
<!ENTITY % CreateTime SYSTEM "CreateTime.dtd">
%CreateTime;
<!ELEMENT PolicyPack (Policy)>
<!ELEMENT Policy (CreateTime, (VulScan | VirusScan))>
<!ATTLIST Policy
    type CDATA #REQUIRED
    version CDATA #REQUIRED
    description CDATA #IMPLIED
    mode CDATA #FIXED "transient"
>
```

维护性操作基本信息见表 A.62。

表 A.62　维护性操作基本信息

参数名	类型	说明	允许取值
name	字符串	操作类型名	见 A.2.3.5 中对应操作类型代码的下划线字符前的部分
version	字符串	安全策略类型版本	见 A.2.3.5 中对应操作类型代码的下划线字符后的部分
description	字符串	描述	

A.3.5.2.2　病毒扫描

本操作用于 SDMI::Policy::PolicyExecutor::fill 方法，见 A.1.2.6。

本操作的 DTD 同 A.3.3.4.4，把其中对 PolicyPack.dtd 的引用改为对 Operation.dtd 的引用即可。

A.3.5.2.3　漏洞扫描

本操作用于 SDMI::Policy::PolicyExecutor::fill 方法，见 A.1.2.6。

```
<?xml version="1.0" encoding="UTF－8"?>
<!－－ VulScan_1.00.dtd －－>
<!ENTITY % PolicyPack SYSTEM "Operation.dtd">
%PolicyPack;
<!ELEMENT VulScan (Action, scan_name)>
<!ATTLIST VulScan
    category CDATA #FIXED "demand"
>
<!ELEMENT Action (#PCDATA)>
<!ATTLIST Action
    category CDATA #FIXED "vulnerability"
>
<!ELEMENT scan_name (#PCDATA)>
```

A.4 安全事件消息格式

生成安全事件消息内容时采用如下的方式：

```
Dict Event;
Event["alert.messageid"] = "……";
Event["alert.create_time"] = "……";
……
```

可填写的安全事件字段见表 A.63。其中字段的类型是指取值类型，在填写安全事件字段时应该总是填写字符串的内容，数字和别的类型全部转化为字符串进行填写。生成的安全事件消息用于SDMI::Event::EventCP::reportEvent 方法的 event 参数，见 A.1.2.6。

表 A.63　安全事件字段表

字段	类型	说明	防火墙	入侵检测	防病毒	主机监控	授权管理	隔离设备
alert.messageid	string	事件标识，其值应是全球唯一的	由安全事件发送方生成的唯一标识					
alert.create_time	string	事件创建的时间。 IDMEF 时间戳，见 A.2.1.2.2。	用 IDMEF 时间戳格式的当前时间填写					
alert.detect_time	string	导致安全事件创建的条件被检测到的时间，有可能早于创建时间。 IDMEF 时间戳，见 A.2.1.2.2。	×	×	×	×	×	×
alert.analyzer_time	string	事件发送时当前系统的时间，安全事件转发一次，该时间就会被调整一次。 IDMEF 时间戳，见 A.2.1.2.2。	×	×	×	×	×	×
alert.analyzer(0).analyzerid	string	事件源标识	SDMI 设备基本管理策略中的 address 元素的值					
alert.analyzer(0).node.address(0).address	string	事件源地址	设备代理的 ip 地址			对应的主机 ip 地址	设备代理的 ip 地址	
alert.analyzer(0).node.address(0).category	string	事件源地址分类	32 bit 的 ip 地址，填写“ipv4-addr”。128bit 的 ip 地址，填写“ipv6-addr”					
alert.analyzer(0).manufacturer	string	事件源厂商，见 A.2.3.6。	填写厂商代码					
alert.analyzer(0).class	string	事件源分类，见 A.2.3.7。	固定填写“Firewall”	固定填写“IDS”	固定填写“Antivirus”	填写对应的主机安全事件源分类代码	固定填写“PME”	固定填写“Isolation”

表 A.63(续)

字段	类型	说明	防火墙	入侵检测	防病毒	主机监控	授权管理	隔离设备
alert.analyzer(0).ostype	string	事件源操作系统类型	×	×	×	×	×	×
alert.analyzer(0).osversion	string	事件源操作系统版本	×	×	×	×	×	×
alert.classification.ident	string	事件类型标识	×	IDS 事件类型代码	防病毒事件类型代码	×	×	应用日志为 1，管理日志为 10
alert.classification.text	string	事件类型	防火墙事件类型，包括“阻止”，“允许”，“管理及运行日志”	IDS 事件类型	防病毒事件类型	主机安全事件类型	授权管理设备事件类型，包括“网络接入控制”或者“应用访问日志”	应用日志以“应用日志_”为前缀的字符串，管理日志以“管理日志_”为前缀的字符串
alert.source(0).interface	string	接口(来源)	源地址通过的接口	×	×	×	×	源地址通过的接口
alert.source(0).spoofed	string	地址伪装(来源)	×	×	×	×	×	×
alert.source(0).node.address(0).address	string	地址(来源)	源地址的 ip 地址	检测到的源地址的 ip 地址	×	ip 防火墙模块填写源地址的 ip 地址	×	源地址的 ip 地址
alert.source(0).node.address(0).netmask	string	掩码(来源)	源地址的 ip 地址掩码	检测到的源地址的 ip 地址掩码	×	×	×	源地址的 ip 地址掩码
alert.source(0).node.address(0).vlan_name	string	VLAN 名(来源)	×	×	×	×	×	×
alert.source(0).node.address(0).vlan_num	int	VLAN 号(来源)	×	×	×	×	×	×
alert.source(0).node.address(0).category	string	地址类型(来源)	当是 32bits 的 ip 地址的时候，填写“ipv4-addr”	当是 32bits 的 ip 地址的时候，填写“ipv4-addr”	×	×	×	当是 32bits 的 ip 地址的时候，填写“ipv4-addr”

表 A.63(续)

字段	类型	说明	防火墙	入侵检测	防病毒	主机监控	授权管理	隔离设备
alert.source(0).user.category	string	用户类型(来源)	×	×	×	×	×	×
alert.source(0).user.user_id(0).name	string	用户名(来源)	×	×	×	×	×	×
alert.source(0).user.user_id(0).number	integer	用户号(来源)	×	×	×	×	×	×
alert.source(0).process.name	string	进程名(来源)	×	×	×	×	×	×
alert.source(0).process.pid	integer	进程号(来源)	×	×	×	×	×	×
alert.source(0).process.path	string	进程路径(来源)	×	×	×	×	×	×
alert.source(0).service.ip_version	string	IP 协议版本(来源)	×	×	×	×	×	×
alert.source(0).service.name	string	服务名(来源)	源地址服务名称	检测到的源地址服务名称	×	×	×	源地址服务名称
alert.source(0).service.port	integer	端口(来源)	源地址服务端口	检测到的源地址服务端口	×	IP 防火墙填写源端口	×	源地址服务端口
alert.source(0).service.protocol	string	协议(来源)	源地址服务协议代码，协议代码是标准的 ip 协议代码	检测到的源地址服务协议代码，协议代码是标准的 ip 协议代码	×	×	×	源地址服务协议代码，协议代码是标准的 ip 协议代码
alert.target(0).interface	string	接口(目标)	目标地址通过的接口	×	×	×	×	目标地址通过的接口
alert.target(0).decoy	string	地址欺骗(目标)	×	×	×	×	×	×
alert.target(0).node.address(0).address	string	地址(目标)	目标地址的 ip 地址	检测到的目标地址的 ip 地址	×	IP 防火墙填写目的 ip 地址	×	目标地址的 ip 地址

表 A.63(续)

字段	类型	说明	防火墙	入侵检测	防病毒	主机监控	授权管理	隔离设备
alert.target(0).node.address(0).netmask	string	掩码(目标)	目标地址的 ip 地址掩码	检测到的目标地址的 ip 地址掩码	×	×	×	目标地址的 ip 地址掩码
alert.target(0).node.address(0).vlan_name	string	VLAN 名(目标)	×	×	×	×	×	×
alert.target(0).node.address(0).vlan_num	integer	VLAN 号(目标)	×	×	×	×	×	×
alert.target(0).node.address(0).category	string	地址类型(目标)	当是 32bits 的 ip 地址的时候，填写“ipv4－addr”	当是32bits的ip地址的时候，填写“ipv4－addr”	×	×	×	当是 32bits 的 ip 地址的时候，填写“ipv4－addr”
alert.target(0).user.category	string	用户类型(目标)	×	×	×	×	×	×
alert.target(0).user.user_id(0).name	string	用户名(目标)	×	×	×	用户姓名	用户姓名	×
alert.target(0).user.user_id(0).ident	string	用户标识(目标)	×	×	×	用户标识	×	×
alert.target(0).user.user_id(0).number	integer	用户号(目标)	×	×	×	×	×	×
alert.target(0).process.name	string	进程名(目标)	×	×	×	进程名，适用于外设控制	×	×
alert.target(0).process.pid	integer	进程号(目标)	×	×	×	×	×	×
alert.target(0).process.path	string	进程路径(目标)	×	×	×	×	×	×
alert.target(0).service.ip_version	string	IP 协议版本(目标)	×	×	×		×	×
alert.target(0).service.name	string	服务名(目标)	目标地址服务名称	检测到的目标地址服务名称	×		×	目标地址服务名称
alert.target(0).service.port	integer	端口(目标)	目标地址服务端口	检测到的目标地址服务端口	×		×	目标地址服务端口

表 A.63(续)

字段	类型	说明	防火墙	入侵检测	防病毒	主机监控	授权管理	隔离设备
alert.target(0).service.protocol	string	协议(目标)	目标地址服务协议代码，协议代码是标准的ip协议代码	检测到的目标地址服务协议代码，协议代码是标准的ip协议代码	×		×	目标地址服务协议代码，协议代码是标准的ip协议代码
alert.target(0).file(0).name	string	文件名(目标)	×	×	病毒感染的文件名	文件名，适用于外设控制	×	×
alert.target(0).file(0).path	string	文件路径(目标)	×	×	病毒感染的文件路径	×	×	×
alert.target(0).file.create_time	时间类型	文件创建时间(目标)	×	×	×	×	×	×
alert.target(0).file.modify_time	时间类型	文件修改时间(目标)	×	×	×	×	×	×
alert.target(0).file.access_time	时间类型	文件访问时间(目标)	×	×	×	×	×	×
alert.target(0).file.data_size	integer	文件大小(目标)	×	×	×	×	×	×
alert.target(0).file.disk_size	integer	存储大小(目标)	×	×	×	×	×	×
alert.assessment.impact.severity	string	严重等级	严重等级，有4个等级“high”、“middle”、“low”、“info”					
alert.assessment.impact.type	string	攻击类型	×	×	×	×	×	×
alert.assessment.impact.completion	string	攻击是否成功	×	×	×	×	×	×
alert.assessment.impact.description	string	影响的描述	×	×	×	×	对应授权管理设备的结果字段	×
alert.assessment.action(0).category	string	采取措施的类型	×	×	×	×	×	×

表 A.63(续)

字段	类型	说明	防火墙	入侵检测	防病毒	主机监控	授权管理	隔离设备
alert.assessment.action(0).description	string	采取措施的的描述	×	×	×	控制所采取的措施：“拒绝”、“允许”	对应授权管理设备的行为字段	×
alert.assessment.confidence.confidence	float	可靠指数	×	×	×	×	×	×
alert.assessment.confidence.rating	string	可靠等级	×	×	×	×	×	×
alert.additional_data(0).data	string	原始日志				存储设备类型，适用于外设控制：“USB存储”、“光驱”、“软驱”、“1394存储”	原始日志	
alert.additional_data(1).data	string	附加信息 1	×	×	×	外部接口类型，适用于外设控制：“打印机”、“串口”	×	应用日志：填写“Pass”或者“Drop” 管理日志：填写操作结果“成功”或者“失败”
alert.additional_data(2).data	string	附加信息 2	×	×	×	外联设备类型：“调制解调器”、“无线网络设备”、“1394网络设备”、“红外设备”、“蓝牙设备”，适用于外联监控	×	应用日志：填写阻止原因 管理日志：造成操作结果的原因
alert.additional_data(3).data	string	附加信息 3	×	×	×	功能异常原因	×	应用日志：业务检查原因描述(应用层属性) 管理日志：操作描述(操作内容)
alert.additional_data(4).data	string	附加信息 4	×	×	×	描述	单位	×

表 A.63(续)

字段	类型	说明	防火墙	入侵检测	防病毒	主机监控	授权管理	隔离设备
alert.additional_data(5).data	string	附加信息 5	×	×	×	×	用户地址	×
alert.additional_data(6).data	string	附加信息 6	×	×	×	×	填写授权控制日志中接入点或者资源对应的字段	×
heartbeat.messageid	uudi	心跳标识						
heartbeat.analyzer(0).analyzerid	string	心跳源标识						
heartbeat.analyzer(0).manufacturer	string	心跳源厂商						
heartbeat.analyzer(0).class	string	心跳源分类						
heartbeat.additional_data(0).data	string	工作状态						

附 录 B
（规范性附录）
用户接口操作逻辑与菜单设置

B.1 操作逻辑

B.1.1 防火墙系统

B.1.1.1 功能划分

防火墙系统的主要功能有安全规则管理、资源管理、网络配置管理、设备参数管理、状态监视、维护工具、辅助功能、帮助和系统管理等。其管理界面的操作逻辑与菜单设计见图 B.1。

B.1.1.2 安全规则管理

安全规则管理的操作逻辑如下：

a) 通过菜单或导航栏选择要进行管理的规则，包括：包过滤、NAT、应用代理、VPN 等；
b) 在主窗口中显示所选类型规则的列表；
c) 通过主窗口中的按钮或右键菜单选择需要进行的操作，可以对规则进行的操作包括：查找、添加、编辑、删除、移动；
d) 以模态弹出式对话框的方式获取用户输入的操作参数，用户确认参数后执行操作并更新主窗口规则列表；
e) 在用户确认操作参数前，能够取消操作；
f) 在用户进行规则参数输入时，如果需要定义新的资源，应弹出资源定义对话框，在用户输入参数并确认后自动添加资源，并返回规则参数对话框。

B.1.1.3 资源管理

资源管理的操作逻辑如下：

a) 通过菜单或导航栏选择要进行管理的资源，包括：地址、协议、服务、时间、带宽、用户等；
b) 在主窗口中显示所选类型资源的列表；
c) 通过主窗口中的按钮或右键菜单选择需要进行的操作，可以对资源进行的操作包括：查找、添加、编辑、删除；
d) 以模态弹出式对话框的方式获取用户输入的操作参数，用户确认参数后执行操作并更新主窗口资源列表；
e) 在用户确认操作参数前，能够取消操作。

B.1.1.4 网络配置管理

网络配置管理的操作逻辑如下：

a) 通过菜单或导航栏选择要进行管理的接口、路由或可用性管理类型，接口类型包括：物理接口、VLAN、网桥接口等，路由类型包括：动态路由、静态路由等，可用性管理类型包括：双机热备、负载均衡、端口同步等；
b) 在主窗口中显示所选类型接口、路由或响应配置的列表；
c) 通过主窗口中的按钮或右键菜单选择需要进行的操作，可以对接口、路由和相关配置进行的操作包括：查找、添加、编辑、删除或停用；
d) 以模态弹出式对话框的方式获取用户输入的操作参数，用户确认参数后执行操作并更新主窗口接口或路由列表；
e) 在用户确认操作参数前，能够取消操作。

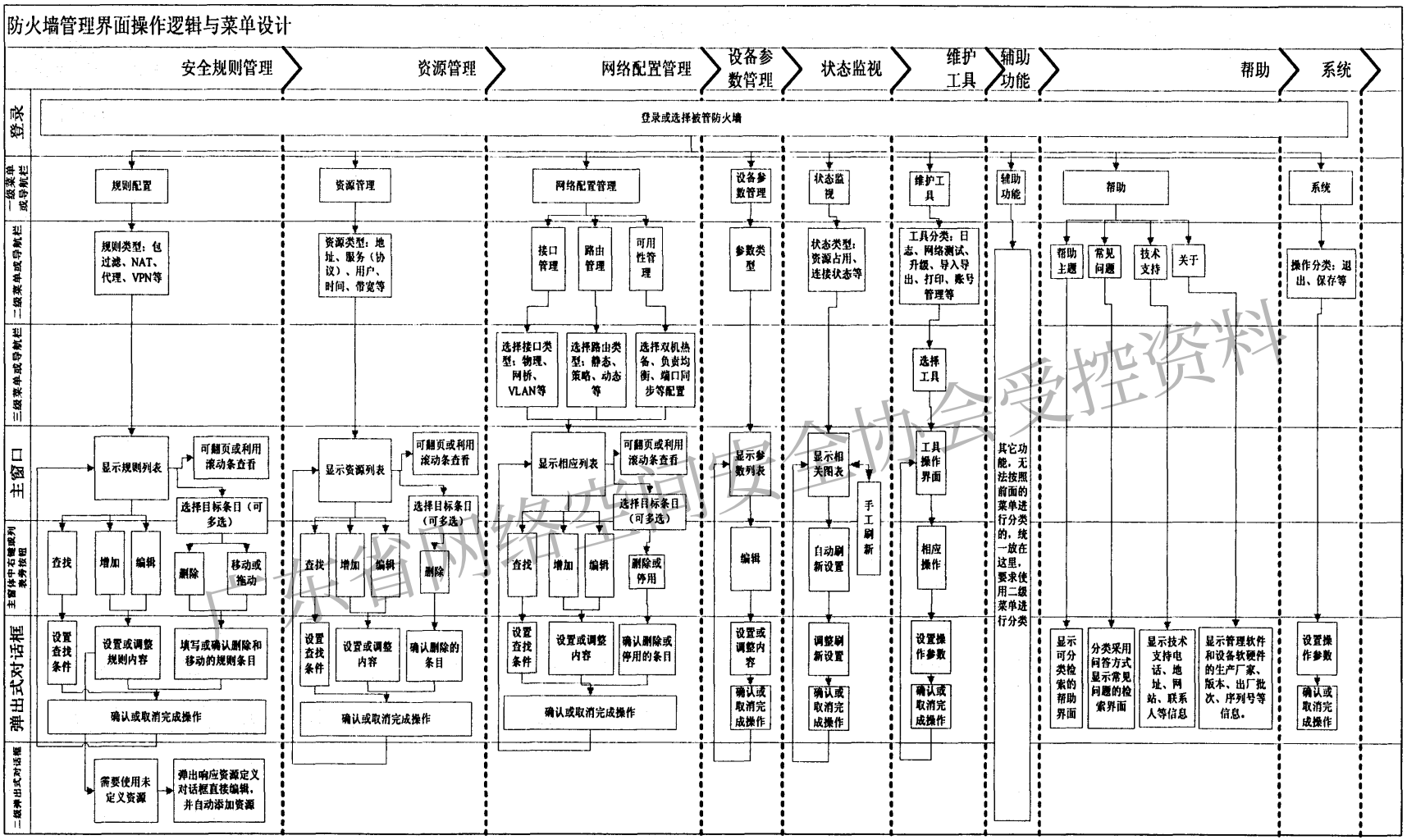

图 B.1　防火墙系统操作逻辑与菜单设计

B.1.1.5 设备参数管理

设备参数管理的操作逻辑如下：

a) 通过菜单或导航栏选择要进行管理的参数类型；

b) 在主窗口中显示所选类型参数的列表；

c) 通过主窗口中的按钮或右键菜单选择需要进行的操作，可以对设备参数进行的操作主要是编辑；

d) 以模态弹出式对话框的方式获取用户输入的操作参数，用户确认参数后执行操作并更新主窗口参数列表；

e) 在用户确认操作参数前，能够取消操作。

B.1.1.6 状态监视

状态监视的操作逻辑如下：

a) 通过菜单或导航栏选择要进行监视的状态类型，包括资源占用、连接状态等；

b) 在主窗口中显示所选类型状态的列表或图表；

c) 通过主窗口中的按钮或右键菜单选择需要进行的操作，可以对状态监视进行的操作包括手工刷新和设置自动刷新间隔；

d) 以模态弹出式对话框的方式获取用户输入的操作参数，用户确认参数后执行操作并更新主窗口的状态列表或图表；

e) 在用户确认操作参数前，能够取消操作。

B.1.1.7 维护工具

维护工具册操作逻辑如下：

a) 通过菜单或导航栏选择要使用的工具，工具的分类包括日志、网络测试、升级、导入导出、打印、账号管理等；

b) 在主窗口中显示所选工具的操作界面和结果显示图表；

c) 通过主窗口中的按钮或右键菜单对工具进行操作；

d) 以弹出式对话框的方式获取用户输入的工具操作参数，用户确认参数后执行操作并更新主窗口的结果显示图表；

e) 在用户确认操作参数前，能够取消操作。

B.1.1.8 辅助功能

辅助功能操作逻辑如下：

a) 防火墙管理中其他无法按照前述小节进行分类的功能，统一归纳放在辅助功能中，可以通过多级(不超过三级)菜单或导航栏分类组织；

b) 操作的主界面和结果应在主窗口中以图表或列表方式显示；

c) 操作参数以弹出式对话框方式获取(对话框的弹出深度不超过二级)。

B.1.1.9 帮助

帮助的操作逻辑如下：

a) 通过菜单或导航栏选择不同的帮助内容，至少应包括帮助主题、常见问题、技术支持、关于等；

b) 以非模态弹出式窗口的方式显示帮助内容；

c) 帮助主题显示可分类检索的帮助信息；

d) 常见问题分类采用问答方式显示常见问题的检索界面；

e) 技术支持显示技术支持电话、地址、网站、联系人等信息；

f) 关于显示管理软件和设备软硬件的生产厂家、版本、出厂批次、序列号等信息。

B.1.1.10 系统

系统操作的操作逻辑如下：

a) 通过菜单或导航栏选择系统操作类型，包括退出、保存等；
b) 以模态弹出式对话框的方式获取用户输入的操作参数，在用户确认后执行相关操作；
c) 在用户确认操作参数前，能够取消操作。

B.1.2 入侵检测系统

B.1.2.1 功能划分

入侵检测系统的主要功能有事件告警管理、策略管理、日志与报表管理、设备参数管理、状态监视、维护工具、辅助功能、帮助和系统管理等。其管理界面的操作逻辑与菜单设计见图 B.2。

B.1.2.2 事件告警管理

事件告警管理的操作逻辑如下：

a) 通过菜单或导航栏选择要显示的事件类型和事件来源，事件类型包括：全部、特征、流量、审计等，事件来源包括：单个引擎、多个引擎、全部引擎等；
b) 在多个并行子窗口或一个主窗口的多个属性页中实时显示符合条件的事件告警列表；
c) 通过事件列表窗口中的按钮或右键菜单选择需要进行的操作，可以进行的操作包括：相关查找、事件帮助、过滤条件、告警方式、新建告警窗口或列表；
d) 当用户选择相关查找操作时，以非模态弹出式对话框的方式获取用户输入的查找条件(查找条件可根据列表中选中的事件自动设置)，用户确认参数后执行操作并弹出新对话框按照统计和详细两个属性页显示查找结果，用户可以选择将结果打印或保存；
e) 当用户选择事件帮助操作时，以非模态对话框方式显示用户选中事件的详细说明和处置建议，用户可以选中打印或保存帮助信息；
f) 当用户选中过滤条件、告警方式或新建告警窗口或列表时，以非模态对话框方式获取用户输入的相关参数(过滤条件可自动根据选中的事件设置)，用户确认后执行相关操作，并更新事件列表窗口；
g) 在用户确认操作参数前，能够取消操作。

B.1.2.3 策略管理

策略管理的操作逻辑如下：

a) 通过菜单或导航栏选择要进行管理的策略类型和操作，策略类型包括：特征事件检测策略、网络审计策略、流量监视策略等，操作包括：下发策略、新建策略模板、编辑已有策略模板等；
b) 当用户选择编辑已有策略模板时，在弹出的非模态窗口中分类显示策略列表(为便于操作可在窗口左侧显示树形分类)；
c) 通过弹出窗口中的按钮或右键菜单选择需要进行的操作，可以进行的操作包括：查找、增加、编辑、删除和下发；
d) 以模态弹出式对话框的方式获取用户输入的操作参数，用户确认参数后执行操作并更新窗口中的策略列表(若用户选择下发操作则执行下发策略的操作逻辑)；
e) 当用户选择新建策略模板时，以弹出式对话框的方式获取新模板的名称、策略衍生源等参数，用户确定后执行编辑已有策略模板的操作逻辑；
f) 当用户选择下发策略时，以弹出式对话框的方式获取目标引擎、欲发策略等参数，用户确定后执行策略下发操作，并在状态窗口中显示策略下发进度和结果；
g) 在用户确认操作参数前，能够取消操作。

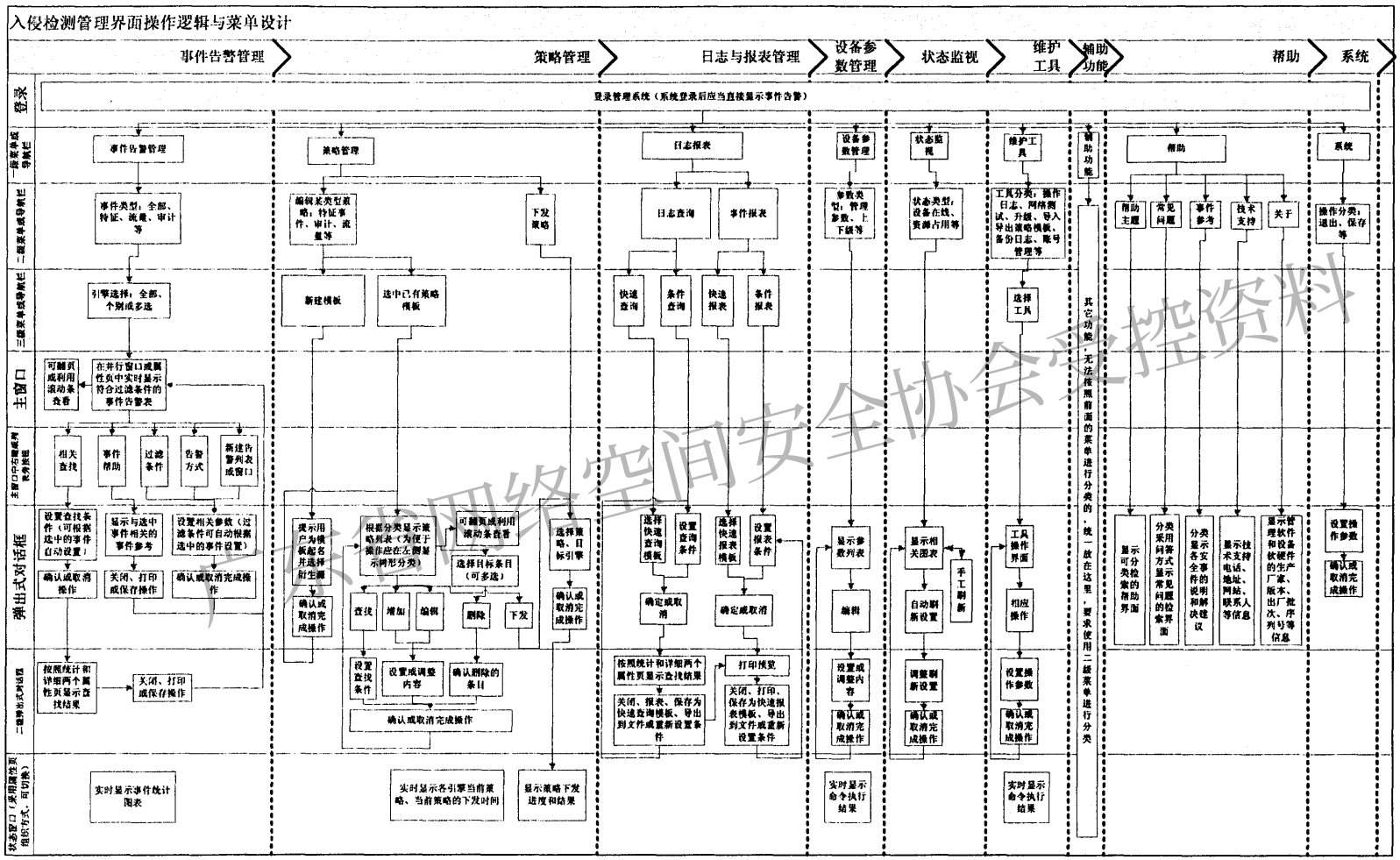

图 B.2　入侵检测系统操作逻辑与菜单设计

B.1.2.4 日志与报表管理

日志与报表管理的操作逻辑如下：

a) 通过菜单或导航栏选择要进行操作类型，包括：快速查询(或报表)、条件查询(或报表)；

b) 在弹出的非模态窗口中请用户选择快速查询(或报表)模块或设置条件查询(或报表)的参数，用户确认后执行查询操作；

c) 查询(或报表)的结果在弹出的新窗口中显示，查询结果按照统计和详细两个属性页显示，报表以打印预览方式显示；

d) 对于查询结果，用户可以选择关闭、报表(执行报表预览操作逻辑)、保存为快速查询模板、导出到文件或重新设置条件(返回条件设置操作逻辑)；

e) 对于报表预览，用户可以选择关闭、打印、保存为快速报表模板、导出到文件或重新设置条件(返回条件设置操作逻辑)；

f) 在用户确认操作参数前，能够取消操作。

B.1.2.5 设备参数管理

设备参数管理的操作逻辑如下：

a) 通过菜单或导航栏选择要进行管理的参数类型，包括管理参数、上下级参数等；

b) 在弹出的非模态窗口中显示所选类型参数的列表；

c) 通过弹出窗口中的按钮或右键菜单选择需要进行的操作，可以对设备参数进行的操作主要是编辑；

d) 以模态弹出式对话框的方式获取用户输入的操作参数，用户确认参数后执行操作并更新窗口参数列表；

e) 在用户确认操作参数前，能够取消操作。

B.1.2.6 状态监视

状态监视的操作逻辑如下：

a) 通过菜单或导航栏选择要进行监视的状态类型，包括资源占用、连接状态等；

b) 在弹出的非模态窗口中显示所选类型状态的列表或图表；

c) 通过弹出窗口中的按钮或右键菜单选择需要进行的操作，可以对状态监视进行的操作包括手工刷新和设置自动刷新间隔；

d) 以模态弹出式对话框的方式获取用户输入的操作参数，用户确认参数后执行操作并更新窗口的状态列表或图表；

e) 在用户确认操作参数前，能够取消操作。

B.1.2.7 维护工具

维护工具操作逻辑如下：

a) 通过菜单或导航栏选择要使用的工具，工具的分类包括操作日志、网络测试、升级、导入导出策略模板、备份日志、账号管理等；

b) 在弹出的非模态窗口中显示所选工具的操作界面和结果显示图表；

c) 通过弹出窗口中的按钮或右键菜单对工具进行操作；

d) 以弹出式对话框的方式获取用户输入的工具操作参数，用户确认参数后执行操作并更新窗口的结果显示图表；

e) 在用户确认操作参数前，能够取消操作。

B.1.2.8 辅助功能

辅助功能操作逻辑如下：

a) 入侵检测管理中其他无法按照前述小节进行分类的功能，统一归纳放在辅助功能中，可以通过多级(不超过三级)菜单或导航栏分类组织；

b) 操作的主界面和结果应于非模态的弹出式窗口中以图表或列表方式显示；

c) 操作参数以弹出式对话框方式获取(对话框的弹出深度不超过二级)。

B.1.2.9 帮助

帮助的操作逻辑如下:

a) 通过菜单或导航栏选择不同的帮助内容,至少应包括帮助主题、常见问题、事件参考、技术支持、关于等;

b) 以非模态弹出式窗口的方式显示帮助内容;

c) 帮助主题显示可分类检索的帮助信息;

d) 常见问题分类采用问答方式显示常见问题的检索界面;

e) 事件参考分类显示各种安全事件的详细说明和处置建议;

f) 技术支持显示技术支持电话、地址、网站、联系人等信息;

g) 关于显示管理软件和设备软硬件的生产厂家、版本、出厂批次、序列号等信息。

B.1.2.10 系统

系统操作的操作逻辑如下:

a) 通过菜单或导航栏选择系统操作类型,包括退出、保存等;

b) 以模态弹出式对话框的方式获取用户输入的操作参数,在用户确认后执行相关操作;

c) 在用户确认操作参数前,能够取消操作。

B.1.3 漏洞扫描系统

B.1.3.1 功能划分

漏洞扫描系统的主要功能有扫描任务管理、报表管理、系统参数管理、状态监视、维护工具、辅助功能、帮助和系统管理等。其管理界面的操作逻辑与菜单设计见图B.3。

B.1.3.2 扫描任务管理

扫描任务管理的操作逻辑如下:

a) 通过菜单或导航栏选择要进行管理的操作,包括:执行任务、新建任务、编辑已有任务、快速扫描等;

b) 当用户选择编辑已有任务时,在主窗口中分类显示策略列表根据分类显示任务列表、任务绑定的引擎和任务当前的执行状态,执行状态包括:停止、暂停、正在执行(显示执行百分比)或等待调度(对于定时执行的任务)(为便于操作应在左侧显示树形分类,分类包括定时扫描、专项扫描等);

c) 通过主窗口中的按钮或右键菜单选择需要进行的操作,可以进行的操作包括:暂定/继续、停止/开始、取消(取消任务的执行及任务与引擎的绑定关系)、查找、编辑、删除和执行;

d) 以模态弹出式对话框的方式获取用户输入的扫描参数,用户确认参数后执行操作并更新窗口中的任务列表(若用户选择执行任务则执行“执行任务”的操作逻辑);

e) 当用户选择新建任务时,以弹出式对话框的方式获取新任务的名称、任务类型等参数,用户确定后执行编辑已有任务的操作逻辑;

f) 当用户选择执行任务时,以弹出式对话框的方式获取目标引擎、欲执行任务等参数,用户确定后执行相关操作;

g) 在执行非即时任务时,状态窗口中显示任务下发进度和结果;在执行即时任务时,采用弹出式对话框显示正在执行的扫描任务和扫描进度,扫描完成后结果显示在主窗口中;

h) 当用户选择快速扫描操作时,以模态弹出式对话框的方式获取用户输入的扫描参数,确认后执行即时扫描任务的操作逻辑;

i) 在主窗口中显示即时扫描结果时,用户可以选择打印、保存或导出扫描结果到文件、返回(返回显示任务列表)和重新扫描(执行快速扫描的操作逻辑)的操作;

j) 在用户确认操作参数前,能够取消操作。

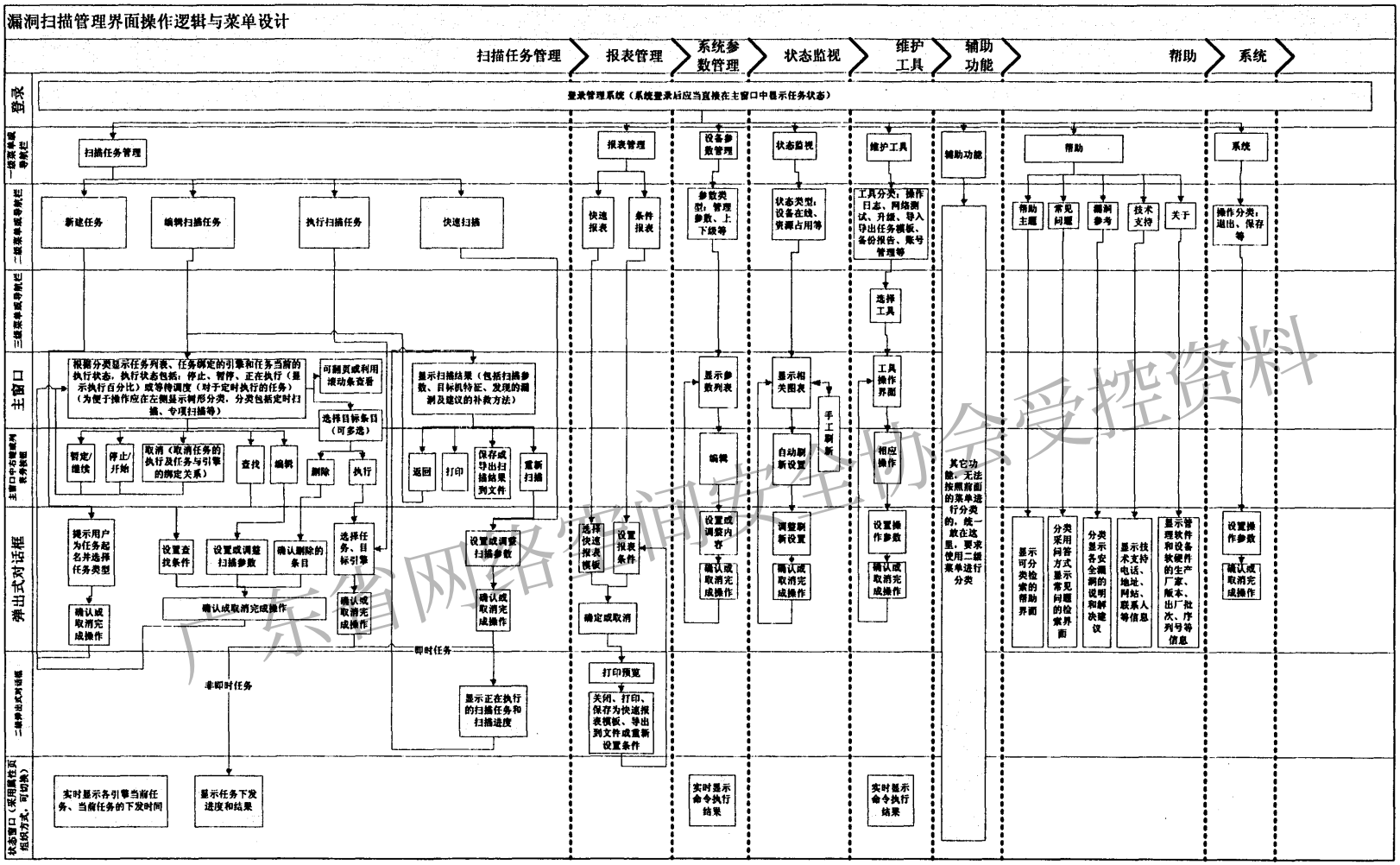

图 B.3　漏洞扫描系统操作逻辑与菜单设计

B.1.3.3 报表管理

报表管理的操作逻辑如下：

a) 通过菜单或导航栏选择要进行的操作类型，包括：快速报表、条件报表；

b) 在弹出的非模态窗口中请用户选择快速报表模块或设置条件报表的参数，用户确认后执行查询操作；

c) 报表的结果在弹出的新窗口中以打印预览方式显示，用户可以选择关闭、打印、保存为快速报表模板、导出到文件或重新设置条件(返回条件设置操作逻辑)；

d) 在用户确认操作参数前，能够取消操作。

B.1.3.4 设备参数管理

设备参数管理的操作逻辑如下：

a) 通过菜单或导航栏选择要进行管理的参数类型，包括管理参数、上下级参数等；

b) 在主窗口中显示所选类型参数的列表；

c) 通过主窗口中的按钮或右键菜单选择需要进行的操作，可以对设备参数进行的操作主要是编辑；

d) 以模态弹出式对话框的方式获取用户输入的操作参数，用户确认参数后执行操作并更新窗口参数列表；

e) 在用户确认操作参数前，能够取消操作。

B.1.3.5 状态监视

状态监视的操作逻辑如下：

a) 通过菜单或导航栏选择要进行监视的状态类型，包括资源占用、连接状态等；

b) 在主窗口中显示所选类型状态的列表或图表；

c) 通过主窗口中的按钮或右键菜单选择需要进行的操作，可以对状态监视进行的操作包括手工刷新和设置自动刷新间隔；

d) 以模态弹出式对话框的方式获取用户输入的操作参数，用户确认参数后执行操作并更新窗口的状态列表或图表；

e) 在用户确认操作参数前，能够取消操作。

B.1.3.6 维护工具

维护工具操作逻辑如下：

a) 通过菜单或导航栏选择要使用的工具，工具的分类包括操作日志、网络测试、升级、导入导出任务模板、备份报告、账号管理等；

b) 在主窗口中显示所选工具的操作界面和结果显示图表；

c) 通过主窗口中的按钮或右键菜单对工具进行操作；

d) 以弹出式对话框的方式获取用户输入的工具操作参数，用户确认参数后执行操作并更新窗口的结果显示图表；

e) 在用户确认操作参数前，能够取消操作。

B.1.3.7 辅助功能

辅助功能操作逻辑如下：

a) 漏洞扫描管理中其他无法按照前述小节进行分类的功能，统一归纳放在辅助功能中，可以通过多级(不超过三级)菜单或导航栏分类组织；

b) 操作的主界面和结果应于非模态的弹出式窗口中以图表或列表方式显示；

c) 操作参数以弹出式对话框方式获取(对话框的弹出深度不超过二级)。

B.1.3.8 帮助

帮助的操作逻辑如下：

a) 通过菜单或导航栏选择不同的帮助内容，至少应包括帮助主题、常见问题、漏洞参考、技术支持、关于等；
b) 以非模态弹出式窗口的方式显示帮助内容；
c) 帮助主题显示可分类检索的帮助信息；
d) 常见问题分类采用问答方式显示常见问题的检索界面；
e) 事件参考分类显示各种安全漏洞的详细说明和处置建议；
f) 技术支持显示技术支持电话、地址、网站、联系人等信息；
g) 关于显示管理软件和设备软硬件的生产厂家、版本、出厂批次、序列号等信息。

B.1.3.9 系统

系统操作的操作逻辑如下：

a) 通过菜单或导航栏选择系统操作类型，包括退出、保存等；
b) 以模态弹出式对话框的方式获取用户输入的操作参数，在用户确认后执行相关操作；
c) 在用户确认操作参数前，能够取消操作。

B.1.4 防病毒系统

B.1.4.1 功能划分

防病毒系统的主要功能有管理控制端操作命令、管理控制端策略管理、管理控制端级联设置、管理控制端工具、管理控制端查询操作、客户端操作命令和客户端策略管理等，其管理界面的操作逻辑与菜单设计见图B.4、图B.5。

B.1.4.2 管理控制端操作命令

操作命令的操作逻辑如下：

a) 通过菜单选择监控命令，可以打开和关闭监控；
b) 在弹出式对话框中可以选择所有监控或者指定监控类型，包括：文件监控、注册表监控、内存监控、邮件监控、网页监控以及引导区监控等等；
c) 还可以通过菜单选择扫描的范围，既可以对全网进行扫描，也可以设置更详细的扫描对象；
d) 在弹出式对话框中显示待扫描的对象，并用复选框对扫描对象进行选择；
e) 以弹出进度条的方式了解扫描对象的执行过程；
f) 扫描完成后在主窗口显示结果，包括发现的病毒、查杀的时间等信息。

B.1.4.3 管理控制端策略管理

策略管理的操作逻辑如下：

a) 通过菜单或导航栏对全网实时监控策略进行编辑；
b) 在弹出式对话框中用复选框进行选择，包括：文件监控、注册表监控、内存监控、邮件监控、网页监控以及引导区监控等等；
c) 通过菜单或导航栏对全网扫描策略进行编辑；
d) 在二级菜单选择扫描方式，包括手动扫描和定时扫描；
e) 通过主窗口中的按钮或右键菜单选择扫描对象，定时扫描模式还要进行扫描方式和时间的设置；
f) 在二级弹出式对话框中弹出进度条显示扫描过程；
g) 通过菜单或导航栏对病毒库升级进行设置，在弹出式对话框中以浏览选定的方式进行病毒库的升级更新；
h) 完成病毒库的更新后，在主窗口可以显示最新病毒库的版本号。

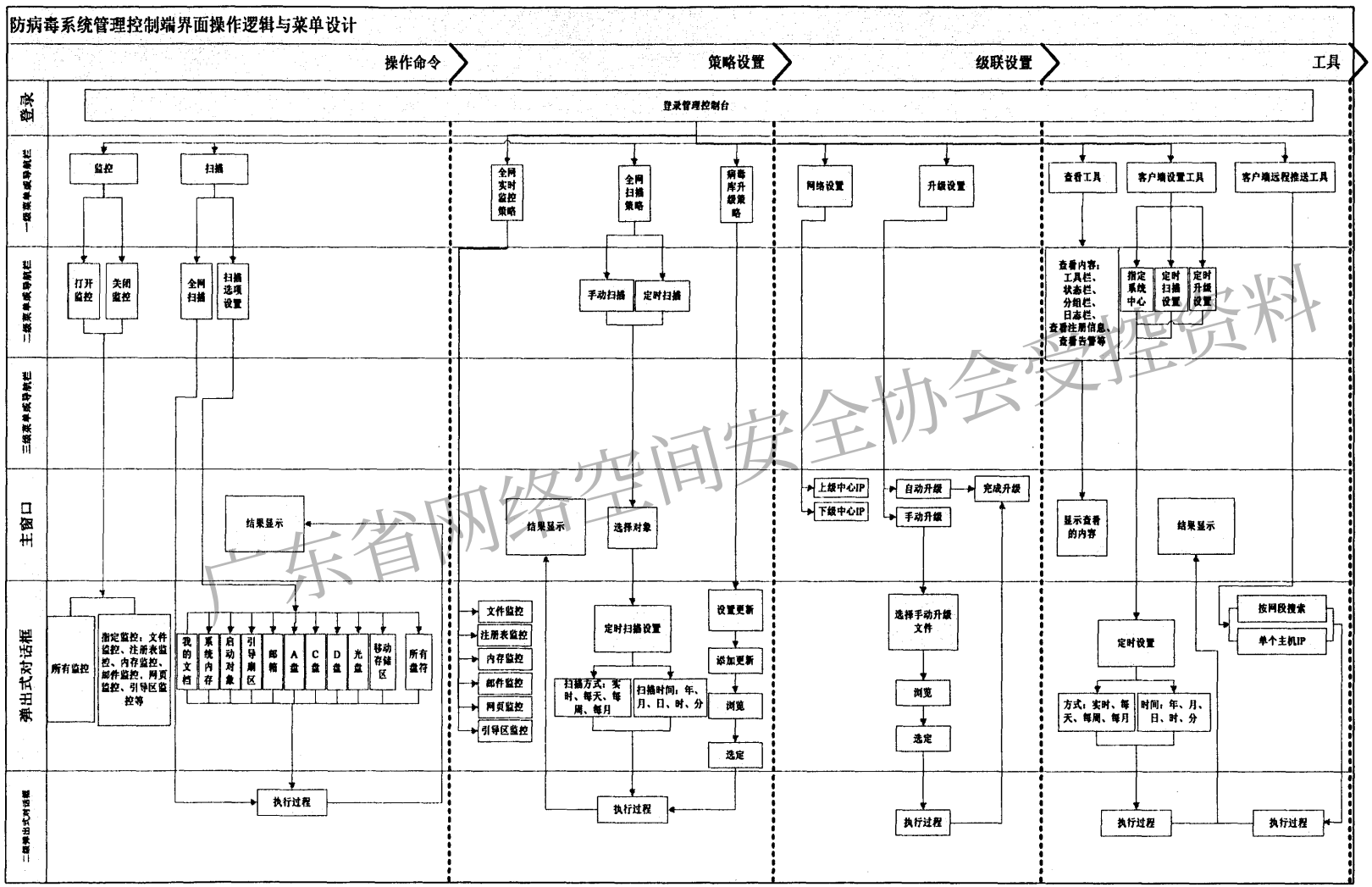

图 B.4　防病毒系统操作逻辑与菜单设计－管理控制端

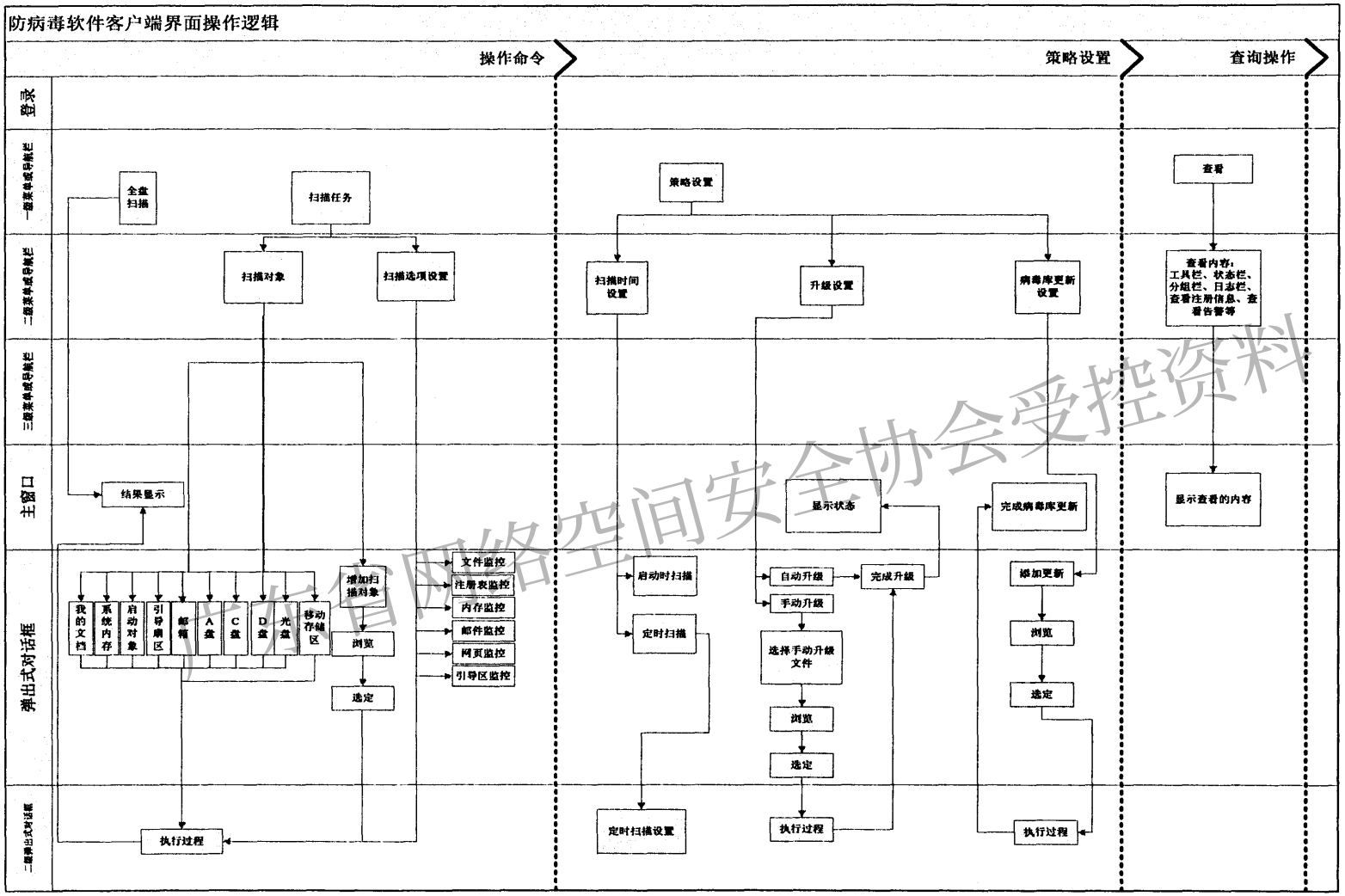

图 B.5　防病毒系统操作逻辑与菜单设计－客户端

B.1.4.4 管理控制端级联设置

级联设置首先对上下级进行指定，然后完成级联的功能，具体操作逻辑如下：

a) 通过菜单或导航栏选择网络设置；

b) 在主窗口中显示的界面上指定上级和下级；

c) 通过主窗口中的按钮或右键菜单选择级联情况下的升级，既可以是自动升级，也可以选择手动升级；

d) 在主窗口显示自动升级后最新版本状态，若为手动升级则在弹出式对话框中以浏览选定的方式选择手动升级文件；

e) 在二级弹出式对话框中显示升级进度，完成后返回主窗口显示最新版本状态。

B.1.4.5 管理控制端工具

工具栏的操作逻辑如下：

a) 通过菜单或导航栏选择要查看工具的类型；

b) 在主窗口中显示所选类型的内容，包括一些告警信息等。

B.1.4.6 管理控制端查询操作

查询的操作逻辑如下：

a) 通过菜单或导航栏选择要查看的类型；

b) 在主窗口中显示所选类型的内容。

B.1.4.7 客户端操作命令

操作命令的操作逻辑如下：

a) 通过菜单选择扫描的范围，可以全盘扫描，也可以根据情况定制扫描任务；

b) 在弹出式对话框中可用复选框对扫描对象进行选择，也可以通过浏览选定的方式添加扫描对象；

c) 在二级弹出式对话框中以弹出进度条的方式了解扫描对象的执行过程；

d) 在二级菜单或导航栏中还可用复选框对扫描选项进行设置，包括文件监控、注册表监控、内存监控、邮件监控、网页监控以及引导区监控等等；

e) 扫描任务完成后在主窗口显示结果，包括发现的病毒、查杀的时间等信息。

B.1.4.8 客户端策略管理

策略管理的操作逻辑如下：

a) 通过菜单或导航栏对扫描时间进行设置，可以选择启动时扫描，也可以设置定时扫描；

b) 在二级弹出式对话框中对定时扫描时间进行设置；

c) 通过菜单或导航栏进行升级设置，可以选择自动升级也可以选择手动升级；

d) 在弹出式对话框中以浏览选定的方式选择手动升级文件；

e) 在二级弹出式对话框中以进度条的方式升级过程；

f) 完成后返回主窗口显示最新版本状态；

g) 通过菜单或导航栏对病毒库的更新设置进行编辑；

h) 在设置更新中以浏览选定的方式添加更新的病毒库；

i) 在二级弹出式对话框中以进度条的方式显示病毒库更新的执行过程；

j) 完成病毒库的更新后，在主窗口可以显示最新病毒库的版本号。

B.1.5 补丁分发系统

B.1.5.1 功能划分

补丁分发系统的主要功能有配置管理、日志与信息查询、维护工具、辅助功能、帮助和系统管理等，其管理界面的操作逻辑与菜单设计见图B.6。

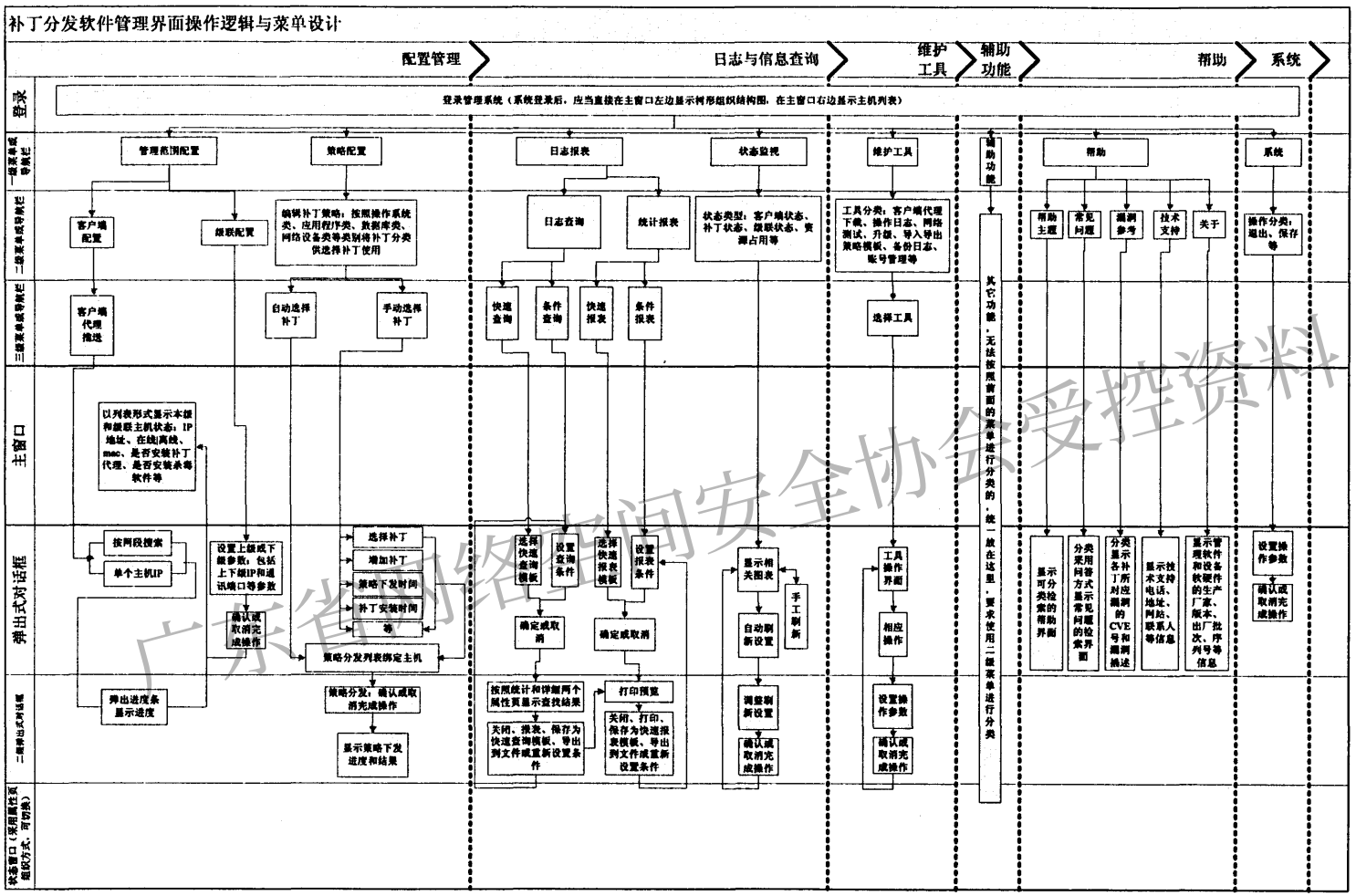

图 B.6　补丁分发系统操作逻辑与菜单设计

B.1.5.2 配置管理

配置管理包括管理范围的配置和策略配置两部分，操作逻辑如下：

a) 通过菜单或导航栏选择管理范围配置，定义需要管理的范围，可以进行本机客户端配置，也可以进行级联控制；

b) 在客户端配置项中可以输入IP地址范围搜索，也可以按IP地址逐个输入主机；在主窗口中显示需要管理的主机，并对这些主机安装客户端，可以批量推送也可以逐台安装；

c) 以弹出进度条的方式了解客户端的安装进度，客户端安装完成之后在主窗口显示主机状态，包括主机是否在线、是否安装杀毒软件以及IP/MAC地址对应等信息；

d) 在级联配置的弹出式对话框项中设置上下级参数，确认或取消完成操作；

e) 通过菜单或导航栏选择策略管理，按照操作系统类、应用程序类、数据库类、网络设备类等类别编辑补丁策略；

f) 在次级菜单或导航栏中编辑策略，既可以自动分发补丁，也可以手动分发补丁；

g) 选定自动分发补丁策略后，在主窗口绑定主机列表进行策略分发；

h) 在弹出式对话框中弹出进度条显示策略分发进度；

i) 选定手动分发补丁策略后，在主窗口中显示策略选项列表，包括选择补丁、增加补丁、策略下发时间以及补丁安装时间等等；

j) 选定策略后通过主窗口中的按钮或右键菜单选择进行策略分发的操作；

k) 以弹出式对话框的方式获取策略和主机列表的绑定；

l) 在二级弹出式对话框中以进度条的方式显示策略分发状态。

B.1.5.3 日志与信息查询

日志与信息查询包括日志报表和状态监视两部分，操作逻辑如下：

a) 通过菜单或导航栏选择日志报表，提供日志查询和统计报表功能，均提供快速查询和条件查询的功能；

b) 在弹出式对话框中，选择快速查询模板或设置查询条件，确定或取消；

c) 在二级弹出式对话框中，按照统计和详细两个属性页显示查找结果，并具备关闭、保存为快速查询或报表模板、导出到文件或重新设置条件等功能；

d) 在一级菜单或导航栏中选择状态监视；

e) 在二级菜单或导航栏中定义客户端状态、补丁状态、级联状态、资源占用等状态类型；

f) 在弹出式对话框中显示相关图表，设置手动刷新或自动刷新等功能。

B.1.5.4 维护工具

维护工具的操作逻辑如下：

a) 通过菜单或导航栏选择维护工具；

b) 在二级菜单或导航栏中进行工具分类，包括客户端代理下载、操作日志、网络测试、升级、导入导出策略模板、备份日志、帐号管理等；

c) 在三级菜单或导航栏选择工具；

d) 在弹出式对话框中弹出工具操作界面，进行相应操作，设置操作参数，确认或取消完成操作。

B.1.5.5 辅助功能

辅助功能操作逻辑如下：

a) 防补丁分发管理中其他无法按照前述小节进行分类的功能，统一归纳放在辅助功能中，可以通过多级(不超过三级)菜单或导航栏分类组织；

b) 操作的主界面和结果应在主窗口中以图表或列表方式显示；

c) 操作参数以弹出式对话框方式获取(对话框的弹出深度不超过二级)。

B.1.5.6 帮助

帮助的操作逻辑如下：

a) 通过菜单或导航栏选择不同的帮助内容，至少应包括帮助主题、常见问题、技术支持、关于等；

b) 以非模态弹出式窗口的方式显示帮助内容；

c) 帮助主题显示可分类检索的帮助信息；

d) 常见问题分类采用问答方式显示常见问题的检索界面；

e) 技术支持显示技术支持电话、地址、网站、联系人等信息；

f) 关于显示管理软件和设备软硬件的生产厂家、版本、出厂批次、序列号等信息。

B.1.5.7 系统

系统操作的操作逻辑如下：

a) 通过菜单或导航栏选择系统操作类型，包括退出、保存等；

b) 以模态弹出式对话框的方式获取用户输入的操作参数，在用户确认后执行相关操作；

c) 在用户确认操作参数前，能够取消操作。

B.2 菜单设置

B.2.1 基本要求

厂家在研制产品时应以各安全系统的操作逻辑定义的最主要功能和共有功能的菜单为基础，适量添加特有功能的菜单项。

B.2.2 防火墙系统主要功能菜单

防火墙系统主要功能菜单见表 B.1。

表 B.1 防火墙系统主要功能菜单

一级菜单	二级菜单	三级菜单	备注
规则配置	包过滤规则	–	
	NAT 规则	–	
	代理规则	–	
	VPN 规则	–	具备 VPN 功能的防火墙可将 VPN 作为一级菜单进行组织
资源管理	地址资源	–	
	服务资源	–	
	用户资源	–	
	时间资源	–	
	带宽资源	–	
网络配置管理	接口管理	物理接口	
		网桥接口	
		VLAN 接口	
	路由管理	静态路由	
		策略路由	
		动态路由	
	可用性管理	双机热备	
		负载均衡	
		端口同步	

表 B.1(续)

一级菜单	二级菜单	三级菜单	备注
设备参数管理	—	—	二级以下菜单由厂家自行拟定
状态监视	资源占用	—	
	连接状态	—	
维护工具	日志	—	
	网络测试	—	
	升级	—	
	导入导出	—	
	打印	—	
	账号管理	—	
辅助功能	—	—	二级以下菜单由厂家自行拟定
帮助	帮助主题	—	
	常见问题	—	
	技术支持	—	
	关于	—	
系统	退出	—	
	保存	—	

B.2.3 入侵检测系统主要功能菜单

入侵检测系统主要功能菜单见表 B.2。

表 B.2 入侵检测系统主要功能菜单

一级菜单	二级菜单	三级菜单	备注
事件告警管理	全部事件	选择引擎	
	特征事件	选择引擎	
	流量事件	选择引擎	
	审计事件	选择引擎	
策略管理	特征事件策略管理	新建模板	
		选中已有策略模板	
	审计策略管理	新建模板	
		选中已有策略模板	
	流量策略管理	新建模板	
		选中已有策略模板	
	下发策略		
日志报表	日志查询	快速查询	
		条件查询	
	事件报表	快速报表	
		条件报表	

表 B.2(续)

一级菜单	二级菜单	三级菜单	备注
设备参数管理	管理参数	–	
	上下级参数	–	
状态监视	设备在线	–	
	资源占用	–	
维护工具	操作日志	–	
	网络测试	–	
	升级	–	
	导入导出策略模板	–	
	备份日志	–	
	账号管理	–	
辅助功能	–	–	二级以下菜单由厂家自行拟定
帮助	帮助主题	–	
	常见问题	–	
	技术支持	–	
	关于	–	
系统	退出	–	
	保存	–	

B.2.4 漏洞扫描系统主要功能菜单

漏洞扫描系统主要功能菜单见表 B.3。

表 B.3 漏洞扫描系统主要功能菜单

一级菜单	二级菜单	三级菜单	备注
扫描任务管理	新建任务	–	
	编辑扫描任务	–	
	执行扫描任务	–	
	快速扫描	–	
报表管理	快速报表	–	
	条件报表	–	
设备参数管理	管理参数	–	
	上下级参数	–	
状态监视	设备在线	–	
	资源占用	–	
维护工具	操作日志	–	
	网络测试	–	
	升级	–	
	导入导出任务模板	–	

表 B.3(续)

一级菜单	二级菜单	三级菜单	备注
维护工具	备份报告	–	
	账号管理	–	
辅助功能	–	–	二级以下菜单由厂家自行拟定
帮助	帮助主题	–	
	常见问题	–	
	技术支持	–	
	关于	–	
系统	退出	–	
	保存	–	

B.2.5 防病毒系统主要功能菜单

防病毒系统主要功能菜单见表 B.4 和表 B.5。

表 B.4 防病毒系统管理端主要功能菜单

一级菜单	二级菜单	三级菜单	备注
监控	打开监控	–	
	关闭监控	–	
扫描	全网扫描	自动分发补丁	
	扫描选项设置	手动选择补丁	
全网实时监控策略	–	–	
	–	–	
全网扫描策略	手动扫描	–	
	定时扫描	–	
病毒库升级策略	–	–	
查看工具	工具栏	–	
	状态栏	–	
	分组栏	–	
	日志栏	–	
	注册信息	–	
	告警	–	
客户端设置工具	指定系统中心	–	
	定时扫描设置	–	
	定时升级设置	–	
客户端远程推送工具	–	–	

表 B.5　防病毒系统客户端主要功能菜单

一级菜单	二级菜单	三级菜单	备注
全盘扫描	打开监控	—	
扫描任务	扫描选项设置	—	
策略设置	扫描时间设置	—	
	升级设置	—	
	病毒库更新设置	—	
查看	状态栏	—	
	分组栏	—	
	日志栏	—	
	注册信息	—	
	告警	—	

B.2.6　补丁分发系统主要功能菜单

补丁分发系统主要功能菜单见表 B.6。

表 B.6　补丁分发系统主要功能菜单

一级菜单	二级菜单	三级菜单	备注
配置管理	管理范围配置	客户端代理推送	
	策略配置	自动分发补丁	
		手动选择补丁	
日志与信息查询	日志报表	日志查询	
		统计报表	
	状态监视	状态类型	
维护工具	客户端代理	—	
	操作日志	—	
	网络测试	—	
	升级	—	
	导入导出策略模板	—	
	备份日志	—	
	帐号管理	—	
辅助功能	—	—	二级以下菜单由厂家自行拟定
帮助	帮助主题	—	
	常见问题	—	
	漏洞参考	—	
	技术支持	—	
	关于	—	
系统	退出	—	
	保存	—	

附 录 C
（资料性附录）
厂商设备代码

C.1 设备厂商子代码

设备厂商子代码参见表 C.1。

表 C.1 设备厂商子代码

设备厂商	简称	代码
上海安纵信息科技有限公司	安纵科技	001
空军装备研究院	空军装备研究院	002
北京网御星云信息技术有限公司	网御星云	003
北京天融信网络安全技术有限公司	天融信	004
北京方正电子政务技术有限公司	方正	005
北京启明星辰信息技术有限公司	启明星辰	006
中国电科第三十研究所	30 所	007
北京中榕基科技发展有限公司	榕基	008
北京瑞星信息技术有限公司	瑞星	009
冠群金辰软件有限公司	冠群金辰	010
国防科技大学	国防科大	011
解放军理工大学	解放军理工大	012
北京北信源自动化技术有限公司	北信源	013

C.2 厂商型号代码

厂商型号代码参见表 C.2。

表 C.2 厂商型号代码

代码	说明
02012001	解放军理工数据库审计系统
03007001	30 所授权管理系统
04008001	榕基网络隐患扫描系统
05006001	启明星辰－IDS 天阗 6.0
05007001	30 卫士鹰眼入侵检测系统
06004001	天融信－NGFW 4000
06003001	网御星云－PowerV
06002001	空军装备研究院网络隔离设备
06007001	30 所网络隔离设备
06011001	国防科大网络隔离设备 1 型

表 C.2(续)

代码	说明
06011002	国防科大网络隔离设备 2 型
07009001	瑞星军队专用版
07010001	KILL-防病毒网络版
08001001	安纵科技-亿仕内网安全管控 v1.1
08013001	北信源补丁管理系统
09002001	网络安全管理系统

中 华 人 民 共 和 国
国家军用标准
网络安全设备管理接口要求
GJB 7554—2012
*
总装备部军标出版发行部出版
（北京东外京顺路 7 号）
总装备部军标出版发行部印刷车间印刷
总装备部军标出版发行部发行
*
开本 880×1230 1/16 印张 8 字数 261 千字
2012 年 10 月第 1 版 2012 年 10 月第 1 次印刷
印数 1—500
*
军标出字第 8735 号 定价 120.00 元

GJB7554-2012 Z