

ICS 35.240

A 90

# GF

公安部计算机信息系统安全产品质量监督检验中心检验规范

MSTL\_JGF\_04-022 0101—2006

---

## 信息安全技术 网际恶意代码控制产品检验规范

2006-01-01 发布

2006-02-01 实施

---

公安部计算机信息系统安全产品质量监督检验中心 发布



## 目 次

前 言 .....	II
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 产品安全功能要求 .....	1
4.1 安全策略控制 .....	1
4.2 自身安全 .....	1
5 产品安全保证要求 .....	2

## 前 言

为了规范全国网际恶意代码控制产品的开发与应用，保障公共信息网络安全，根据公安部公共信息网络安全监察局的要求，本规范对网际恶意代码控制产品提出了安全功能要求和保证要求，作为对其进行检测的依据。

本规范由中华人民共和国公安部公共信息网络安全监察局批准。

本规范起草单位：公安部计算机信息系统安全产品质量监督检验中心。

公安部计算机信息系统安全产品质量监督检验中心负责对本规范的解释、提升和更改。

# 信息安全技术 网际恶意代码控制产品检验规范

## 1 范围

本规范规定了网际恶意代码控制产品的安全功能要求和安全保证要求。  
本规范适用于网际恶意代码控制产品的开发及检测。

## 2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 18336.3—2001 信息技术 安全技术 信息技术安全性评估准则 第3部分：安全保证要求（idt ISO/IEC 15408-3:1999）

## 3 术语和定义

### 3.1 安全策略控制 Security Policy Enforcement

安全策略控制是网络安全防范和保护的主要策略，它的主要任务是保证网络资源不被非法使用，避免网络蠕虫肆虐与危害，安全策略控制的目的在于使不合乎安全策略的用户无法使用网络的便利性。

### 3.2 网际恶意代码 Malice Code of Network

网际恶意代码是一种通过网络传播的程序，通过把代码镶嵌到另一段程序中，从而达到破坏被感染电脑数据、运行具有入侵性的程序、破坏被感染电脑安全性的目的。按传播方式与功能特点，恶意代码可以分成四类：病毒，木马，蠕虫和移动代码。本规范所规定的网际恶意代码，不包括病毒。

## 4 产品安全功能要求

### 4.1 安全策略控制

#### 4.1.1 安全策略识别

应能针对常见网际恶意代码的攻击进行用户的安全策略配置。

#### 4.1.2 访问限制

有且只有符合防常见网际恶意代码安全策略配置的用户/主机才能访问外网资源。

#### 4.1.3 系统接入

宜提供网桥式部署方式接入网络的能力。

#### 4.1.4 恶意代码控制

——应从内外两个方向对常见网际恶意代码进行过滤控制，以防止上述恶意代码的网际传播。

——对恶意代码传播所造成的常见攻击，如 DoS、DDoS，产品也应具备一定的保护功能。

### 4.2 自身安全

#### 4.2.1 符合规定的加密操作

a) 如果支持远程管理，应能够通过加密来保护远程管理对话；

b) 如果用户必须通过网络访问特定信息，应能够通过加密来保护远程访问会话。

#### 4.2.2 管理员身份鉴别

应保证只有授权管理员和可信主机才有权使用产品的管理功能，对授权管理员和可信主机应进行身份鉴别。

#### 4.2.3 管理员权限

- a) 管理员属性修改（更改密码等）；
- b) 制定和修改访问控制安全策略。

#### 4.2.4 管理权限划分

应对划分不同的安全管理角色，对产品进行合理的权限分配。

#### 4.2.5 日志功能

##### 4.2.5.1 日志数据生成

- a) 应能对下列事件生成日志：
  - 对不符合安全策略的用户进行审计跟踪；
  - 对管理者的身份鉴别结果应进行审计跟踪；
- b) 应在每一个日志记录中记录事件发生的日期和时间、事件描述。

##### 4.2.5.2 日志管理

应提供下列日志管理功能：

- a) 只允许授权管理员访问日志记录；
- b) 提供对日志记录的查询功能。

#### 4.2.6 自动升级

应对至少提供对策略库的远程自动升级功能。

### 5 产品安全保证要求

保证要求按 GB/T 18336.3—2001 第二级执行。

---