

编号：CNCA-11C-084:2009

# 信息安全产品强制性认证实施规则

## 入侵检测系统（IDS）产品

2009-04-27 发布

2009-05-01 实施

---

中国国家认证认可监督管理委员会发布

# 目 录

1. 适用范围.....	1
2. 认证模式.....	1
3. 认证的基本环节.....	1
3.1 认证申请及受理 .....	1
3.2 型式试验委托及实施 .....	1
3.3 初始工厂检查 .....	1
3.4 认证结果评价与批准 .....	1
3.5 获证后监督 .....	1
4. 认证实施.....	1
4.1 认证程序 .....	1
4.2 认证申请及受理 .....	2
4.3 型式试验委托及实施 .....	3
4.4 初始工厂检查 .....	4
4.5 认证结果评价与批准 .....	5
4.6 获证后监督 .....	6
5. 认证证书.....	7
5.1 认证证书的保持 .....	7
5.2 认证证书覆盖产品的扩展 .....	8
5.3 认证证书的暂停、注销和撤销 .....	8
6. 强制性产品认证标志的使用.....	8
6.1 准许使用的标志样式 .....	8
6.2 变形认证标志的使用 .....	8
6.3 加施方式 .....	8
6.4 标志位置 .....	9
7. 收费.....	9
附件 1: .....	10
附件 2: .....	11
附件 3: .....	14
附件 4: .....	15
附件 5: .....	16

## 1. 适用范围

本规则所指的入侵检测系统指通过对计算机网络或计算机系统中的若干关键点收集信息并对其进行分析，发现违反安全策略的行为和被攻击迹象的软件或软硬件组合。

本规则适用的产品范围为：（1）网络型入侵检测系统；（2）主机型入侵检测系统。

拟用于涉密信息系统的上述产品，按照国家有关保密规定和标准执行，不适用本规则。

## 2. 认证模式

型式试验 + 初始工厂检查 + 获证后监督

## 3. 认证的基本环节

3.1 认证申请及受理

3.2 型式试验委托及实施

3.3 初始工厂检查

3.4 认证结果评价与批准

3.5 获证后监督

## 4. 认证实施

### 4.1 认证程序

申请方可选择集中受理或分段受理两种方式中任何一种进行认证证书申请，两种方式下获得的证书是等效的。

#### 4.1.1 集中受理流程

申请方向指定的认证机构申请认证，认证机构对申请产品进行单元划分并审查申请资料，确认合格后向实验室（由申请方自主从指定实验室名单中选取）安排检测任务。实验室依据相关产品强制性认证实施规则进行检测，并在完成检测后向认证机构提交完整的检测报告。认证机构对检测报告审查合格后，由认证机构进行初始工厂检查。认证机构对型式试验、

初始工厂检查结果进行综合评价，评价合格后向申请方颁发认证证书。认证机构组织对获证后的产品进行定期的监督。

#### 4.1.2 分段受理流程

申请方自主从指定实验室名单中选取实验室，并向实验室提交相关申请材料。实验室对申请产品进行单元划分，审查并确认所需资料合格后，依据认证实施规则进行检测，检测通过后向认证机构提交检测报告。检测报告经认证机构确认合格后，申请方向认证机构提交认证所需资料。认证机构审查并确认所需资料合格后，由认证机构进行初始工厂检查。认证机构对型式试验、初始工厂检查结果进行综合评价，评价合格后向申请方颁发认证证书。认证机构组织对获证后的产品进行定期的监督。

#### 4.2 认证申请及受理

##### 4.2.1 认证的单元划分

###### 4.2.1.1 网络型入侵检测系统

按产品型号/版本申请认证，若产品的信息安全关键件实现方式相同的可作为一个单元申请认证，但具有不同带宽网络接口的产品，应分开申请认证。

以多于一个型号/版本的产品为同一认证单元申请认证时，申请方应提交同一认证单元中型号/版本间的差异说明及相关自测报告。

###### 4.2.1.2 主机型入侵检测系统。

按产品型号/版本申请认证，若产品的信息安全关键件实现方式相同的可作为一个单元申请认证，但支持不同主机环境（如操作系统、应用软件、数据库系统等）的产品，应分开申请认证。

以多于一个型号/版本的产品为同一认证单元申请认证时，申请方应提交同一认证单元中型号/版本间的差异说明及相关自测报告。

##### 4.2.2 申请时需提交的文件资料

申请方在申请产品认证时，提交的文件资料应至少包含以下内容：

1. 申请方情况：

- 1) 基本情况介绍；
- 2) 相关资质证明材料（复印件）；
- 3) 质量体系方面有关的文件；
- 4) 申请方声明。

2. 产品相关说明：

- 1) 中文产品功能说明书和/或使用手册；
- 2) 认证标准的适用性说明；
- 3) 产品研制主要技术人员情况表；
- 4) 产品测试技术人员情况表；
- 5) 产品测试使用的主要设备表（如适用）；
- 6) 中文铭牌和警告标记（如适用）；
- 7) 同一认证单元中型号/版本间的差异说明及相关自测报告（如适用）。

3. 与申请认证级别相对应的安全保证要求的说明，包括以下方面：

- 1) 配置管理；
- 2) 交付和运行；
- 3) 开发；
- 4) 指导性文档；
- 5) 生命周期支持；
- 6) 测试；
- 7) 脆弱性评定。

4.3 型式试验委托及实施

4.3.1 型式试验的送样

4.3.1.1 型式试验送样的原则

认证单元中只有一个型号/版本的，送该型号/版本的样品。

以多于一个型号/版本的产品作为同一认证单元申请认证时，应从中选取典型的型号/版本作为送样产品。

申请第二级（含）以上的网络型产品在送样时，应同时提供该产品的联动设备及相关说明性文档。

#### 4.3.1.2 送样要求和数量

型式试验的样品由申请方负责选送，并对选送样品负责。一般每种产品送样 2 套。

#### 4.3.1.3 型式试验样品及相关资料的处置

认证结束后，申请方可向实验室申请取回型式试验样品，相关申请资料由认证机构、实验室妥善处置。

#### 4.3.2 测评标准和项目

测评依据的标准为：

GB/T 20275 《信息安全技术 入侵检测系统技术要求和测试评价方法》（基于 GB/T 18336 《信息技术 安全技术 信息安全技术评估准则》的通用要求）。

测评项目见附件 2、附件 3。

#### 4.3.3 型式试验报告的提交

型式试验完成后，实验室出具型式试验报告并提交给认证机构。

#### 4.4 初始工厂检查

##### 4.4.1 检查内容

初始工厂检查的内容为信息安全保证能力、质量保证能力和产品一致性检查。

##### 4.4.1.1 信息安全保证能力检查

由认证机构派检查员对工厂按照《入侵检测系统产品强制性认证安全保障评估项目》（见附件 3）进行信息安全保证能力检查。

##### 4.4.1.2 质量保证能力检查

由认证机构派检查员对工厂按照《质量保证能力基本要求》（附件 5）及认证机构制定的补充检查要求（适用时）进行检查。

#### 4.4.1.3 产品一致性检查

初始工厂检查时，应在生产现场对申请认证的产品进行一致性检查。重点核实以下内容：

- 1) 认证产品的铭牌、包装上所标明的及运行时所显示的产品名称、型号/版本号与型式试验报告上所标明的内容是否一致；
- 2) 非认证的产品是否违规标贴了认证标识。

#### 4.4.2 初始工厂检查时间

一般情况下，认证机构对 4.2.2 中的资料进行审查并在型式试验完成后，再进行初始工厂检查。特殊情况时，型式试验和初始工厂检查也可以同时进行。

初始工厂检查时间根据所申请认证产品的单元数量确定，并适当考虑生产厂的规模及产品的安全级别，一般每个生产厂为 2 至 4 个人日。

### 4.5 认证结果评价与批准

#### 4.5.1 认证结果评价与批准

认证机构负责对型式试验、初始工厂检查结果进行综合评价，评价合格的，由认证机构对申请方颁发认证证书（每一个认证单元颁发一个认证证书）。如认证决定过程中发现不符合认证要求项，允许限期（不超过 3 个月）整改，如期完成整改后，认证机构采取适当方式对整改结果进行确认，重新执行认证决定过程。

#### 4.5.2 认证时限

认证时限是指自申请被正式受理之日起至颁发认证证书时止所实际发生的工作日，其中包括型式试验时间、初始工厂检查及提交报告时间、认证结论评定和批准时间以及证书制作时间。

型式试验时间一般不超过 40 个工作日（因检测项目不合格，进行整改

和复试的时间不计算在内，整改时间一般不超过 3 个月)。一般在型式试验报告提交后 30 个工作日内安排初始工厂检查。初始工厂检查时间根据所认证产品的单元数量确定，并适当考虑生产厂的生产规模及产品的安全级别，一般为 2 至 4 个人日。初始工厂检查后提交报告时间一般为 5 个工作日，以检查员完成现场检查，收到并确认工厂递交的不合格纠正措施报告之日起计算。

认证结论评定、批准时间以及证书制作时间共计不超过 5 个工作日。

## 4.6 获证后监督

### 4.6.1 监督的频次

4.6.1.1 从获证后第 12 个月起进行第一次获证后监督，此后每 12 个月进行一次获证后监督。必要情况下，认证机构可采取事先不通知的方式对生产厂实施监督。

4.6.1.2 若发生下述情况之一可增加监督频次：

1) 获证产品出现严重质量问题时，或者用户提出投诉并经查实为证书持有者责任时；

2) 认证机构有足够理由对获证产品与本规则中规定的标准要求符合性提出质疑时；

3) 有足够信息表明工厂因组织机构、生产条件、质量管理体系等发生变更，从而可能影响产品质量时。

### 4.6.2 监督的内容

获证后监督的方式采用信息安全保证能力与质量保证能力的复查和认证产品一致性检查。必要时可以抽取样品送实验室检测，需要进行抽样检测时，抽样检测的样品应在工厂生产的产品中（包括生产线、仓库、市场）随机抽取。产品抽样检测的数量为 2 套。本认证实施规则中涉及的检测项均可作为监督检测项目，认证机构可要求针对不同产品的不同情况进行部分或全部项目的检测。对抽取样品的检测由认证机构指定的实验室在 20 个

工作日内完成。

认证机构根据《入侵检测系统产品强制性认证安全保证评估项目》（见附件 3）、《质量保证能力基本要求》（见附件 5）对工厂进行监督复查。《质量保证能力基本要求》规定的第 1、2 条是每次监督复查的必查项目，其他项目可以选查。每四年内至少覆盖附件 3、附件 5 中所包括的全部项目。另外，应对产品的变更情况进行核查。

工厂监督检查时间根据获证产品的单元数量确定，并适当考虑工厂的生产规模及安全级别，一般为 1 至 3 个人日。

#### 4.6.3 获证后监督结果的评价

监督复查合格后，可以继续保持认证证书、使用认证标志。对监督复查时发现的不符合项应在 3 个月内完成纠正措施。逾期将撤销认证证书、停止使用认证标志，并对外公告。

### 5. 认证证书

#### 5.1 认证证书的保持

##### 5.1.1 证书的有效性

本规则覆盖产品的认证证书不规定截止日期。证书的有效性依赖认证机构定期的监督获得保持。

##### 5.1.2 认证产品的变更

###### 5.1.2.1 变更的申请

获证后的产品，如果其产品的信息安全关键件未发生变化而型号/版本变化，或生产厂、证书持有者等发生变化时，应向认证机构提出变更申请。

由信息安全关键件的变化引起型号/版本变化时，应重新申请认证。

###### 5.1.2.2 变更申请的评价与批准

认证机构根据变更的内容和提供的资料进行评价，确定已获证产品的变化属于以下何种情况，并根据具体情况采取相应措施。

1) 由产品非信息安全关键件变化引起型号/版本变化，且不需补充型

式试验和/或工厂检查时，经审核后予以变更；

2) 由产品非信息安全关键件变化引起型号/版本变化，且需补充型式试验和/或工厂检查时，应在完成型式试验和/或工厂检查并经认证评价合格后方予以变更；

3) 发生其它变化时，如生产厂、证书持有者等，经审核后予以变更。

## 5.2 认证证书覆盖产品的扩展

### 5.2.1 认证证书覆盖产品扩展申请

认证证书持有者需要增加已经获得认证产品的认证范围时，应向认证机构提出扩展申请。

### 5.2.2 认证证书覆盖产品扩展的评价与批准

认证机构应核查扩展产品与原认证产品的一致性，确认原认证结果对扩展产品的有效性，需要时应针对差异做补充型式试验和/或工厂检查，并根据认证证书持有者的要求单独颁发认证证书或换发认证证书。

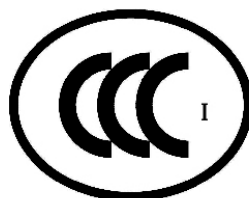
## 5.3 认证证书的暂停、注销和撤销

按《强制性产品认证证书注销、暂停和撤销实施规则》的要求执行。在认证证书暂停期间及认证证书注销和撤销后，企业不得继续使用证书。

## 6. 强制性产品认证标志的使用

证书持有者必须遵守《强制性产品认证标志管理办法》的规定。

### 6.1 准许使用的标志样式



### 6.2 变形认证标志的使用

本规则覆盖的产品不允许使用任何形式的变形认证标志。

### 6.3 加施方式

可以采用国家统一印制的标准规格标志、模压或铭牌印刷三种方式中的任何一种。

采用模压或铭牌印刷时,其使用方案应报国家认证认可监督管理委员会批准的强制性产品认证标志发放与管理机构核准。

#### 6.4 标志位置

应在产品本体的铭牌附近加施认证标志。

软件产品应在其软件包装/载体上加施认证标志,如该软件产品不使用包装/载体,则应在软件使用的《许可协议》中的显著位置明确该产品已获中国强制性产品认证(CCC认证)。

### 7. 收费

收费由认证机构、实验室按国家有关规定统一收取。

附件 1:

### 入侵检测系统产品强制性认证单元划分

产品名称及形态		单元划分原则	认证依据标准	送样数量
入侵检测系统	网络型入侵检测系统	<p>按产品型号/版本申请认证,若产品的信息安全关键件实现方式相同的可作为一个单元申请认证,但具有不同带宽网络接口的产品,应分开申请认证。</p> <p>以多于一个型号/版本的产品为同一认证单元申请认证时,申请方应提交同一认证单元中型号/版本间的差异说明及相关自测报告。</p>	GB/T 20275 《信息安全技术 入侵检测系统技术要求和测试评价方法》	2 套
	主机型入侵检测系统	<p>按产品型号/版本申请认证,若产品的信息安全关键件实现方式相同的可作为一个单元申请认证,但支持不同主机环境(如操作系统、应用软件、数据库系统等)的产品,应分开申请认证。</p> <p>以多于一个型号/版本的产品为同一认证单元申请认证时,申请方应提交同一认证单元中型号/版本间的差异说明及相关自测报告。</p>	GB/T 20275 《信息安全技术 入侵检测系统技术要求和测试评价方法》	

附件 2:

入侵检测系统产品强制性认证检测项目

安全级别	检测项	认证依据标准
第一级	产品功能要求 数据探测 入侵分析 入侵响应 管理控制 检测结果处理 产品灵活性 性能指标 安全要求 身份鉴别 用户管理 事件数据安全 通信安全 产品自身安全	GB/T 20275 《信息安全技术 入侵检测系统技术要求和测试评价方法》

<p>第二级</p>	<p>安全功能要求</p> <ul style="list-style-type: none"> <li>数据探测</li> <li>入侵分析</li> <li>入侵响应</li> <li>管理控制</li> <li>检测结果处理</li> <li>产品灵活性</li> <li>性能指标</li> </ul> <p>安全要求</p> <ul style="list-style-type: none"> <li>身份鉴别</li> <li>用户管理</li> <li>安全审计</li> <li>事件数据安全</li> <li>通信安全</li> <li>产品自身安全</li> </ul>	<p>GB/T 20275 《信息安全技术 入侵检测系统技术要求和测试评价方法》</p>
------------	--	--

<p>第三级</p>	<p>安全功能要求</p> <ul style="list-style-type: none"> <li>数据探测</li> <li>入侵分析</li> <li>入侵响应</li> <li>管理控制</li> <li>检测结果处理</li> <li>产品灵活性</li> <li>性能指标</li> </ul> <p>安全要求</p> <ul style="list-style-type: none"> <li>身份鉴别</li> <li>用户管理</li> <li>安全审计</li> <li>事件数据安全</li> <li>通信安全</li> <li>产品自身安全</li> </ul>	<p>GB/T 20275 《信息安全技术 入侵检测系统技术要求和测试评价方法》</p>
------------	--	--

附件 3:

入侵检测系统产品强制性认证安全保证评估项目

安全级别	评估项	认证依据标准
第一级	配置管理 交付和运行 开发 指导性文档 生命周期支持 测试	GB/T 20275 《信息安全技术 入侵检测系统技术要求和测试评价方法》中第一级的相应要求
第二级	配置管理 交付和运行 开发 指导性文档 生命周期支持 测试 脆弱性评定	GB/T 20275 《信息安全技术 入侵检测系统技术要求和测试评价方法》中第二级的相应要求
第三级	配置管理 交付和运行 开发 指导性文档 生命周期支持 测试 脆弱性评定	GB/T 20275 《信息安全技术 入侵检测系统技术要求和测试评价方法》中第三级的相应要求

附件 4:

入侵检测系统产品的信息安全关键件

安全级别	关键件
第一级	数据探测与入侵分析模块、入侵响应模块、检测结果处理模块、自身安全管理模块
第二级	数据探测与入侵分析模块、入侵响应模块、检测结果处理模块、自身安全管理模块、审计模块
第三级	数据探测与入侵分析模块、入侵响应模块、检测结果处理模块、自身安全管理模块、审计模块

## 附件 5:

### 质量保证能力基本要求

为保证批量生产的认证产品与型式试验样品的一致性，工厂应满足本文件规定的质量保证能力基本要求。

#### 1. 职责和资源

##### 1.1 职责

工厂应规定与质量活动有关的各类人员职责及相互关系，且工厂应在组织内指定一名质量负责人，无论该成员在其他方面的职责如何，应具有以下方面的职责和权限：

- a) 负责建立满足本文件要求的质量体系，并确保其实施和保持；
- b) 确保加贴强制性认证标志的产品符合认证标准的要求；
- c) 建立文件化的程序，确保认证标志的妥善保管和使用；
- d) 建立文件化的程序，确保不合格品和获证产品变更后未经认证机构确认，不加贴强制性认证标志。

质量负责人应具有充分的能力胜任本职工作。

##### 1.2 资源

工厂应配备必须的生产设备和检测设备以满足稳定生产符合本规则中规定的标准要求的产品；应配备相应的人力资源，确保从事对产品质量有影响工作的人员具备必要的能力；建立并保持适宜产品生产、试验、储存等必备的环境。

#### 2. 强制性认证产品的一致性

- a) 工厂应对现场的产品与型式试验样品的一致性进行控制，以使认证

产品持续符合规定的要求；

b) 工厂应建立产品变更控制程序，认证产品的变更在实施前应向认证机构申报并获得批准后方可执行。

### 3. 强制性认证产品外购部件或外包软件模块管理

#### 3.1 外购部件供应商或软件模块的外包商的控制

a) 工厂应制定外购部件供应商或软件模块的外包商的选择、评定和日常管理的程序，以确保供应商提供的部件或软件外包商提供的软件模块满足要求；

b) 工厂应保存对供应商或软件外包商的选择评价和日常管理记录。

#### 3.2 外购部件或外包软件模块的验证

a) 工厂应建立并保持对供应商提供的部件或软件外包商提供的软件模块的验证程序及定期确认程序，以确保部件或软件模块满足认证所规定的要求；

b) 工厂应保存部件或外包软件模块，或者它们的验证记录、确认记录及供应商或软件外包商提供的合格证明及有关数据等。