ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20945—2007

信息安全技术　信息系统安全审计产品技术要求和测试评价方法

**Information security technology—
Technical requirements, testing and evaluation approaches
for information system security audit products**

2007-06-13 发布　　2007-12-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准的附录A是资料性附录。

本标准由全国信息安全标准化技术委员会提出并归口。

本标准起草单位：北京中科网威信息技术有限公司、公安部计算机信息系统安全产品质量监督检验中心、上海汉邦京泰数码技术有限公司。

本标准主要起草人：肖江、叶小列、刘宝旭、王晓箴、顾健、沈亮、陆中威、王贤蔚、王鸣。

引　言

信息系统安全审计产品为评估信息系统的安全性和风险和完善安全策略制定提供审计数据和审计服务支撑，从而达到保障信息系统正常运行的目的。同时，信息系统安全审计产品对信息系统各组成要素进行事件采集，将采集数据进行自动综合和系统分析，能够提高信息系统安全管理的效率。

本标准规定了安全审计产品的基本技术要求和扩展技术要求，提出了该类产品应达到的安全目标，并给出了该类产品的基本功能、增强功能和安全保证要求。

本标准规定了安全审计产品的测评方法，包括安全审计产品测评的内容和测评功能目标，给出了产品基本功能、增强功能和安全保证要求必须达到的具体目标。

本标准的目的是规范设计者如何设计和实现安全审计产品，并为安全审计产品的测评和应用提供技术支持和指导。

本标准用以规范设计者如何设计和实现安全审计产品，并为安全审计产品的测评和应用提供技术支持和指导。

本标准规定了基本型和增强型安全审计产品的技术要求以及测评方法，给出了该类产品应达到的安全功能要求和安全保证要求的具体目标。

信息安全技术 信息系统安全审计产品技术要求和测试评价方法

1 范围

本标准规定了信息系统安全审计产品技术要求(安全功能要求、自身安全要求、性能要求和保证要求)和对应的测评方法。

本标准适用于信息系统审计产品的开发、测评和应用。

2 规范性引用文件

下列文件中的条款通过本部分的引用而成为本部分的条款。凡是注日期的引用文件,其随后所有的修改单(不包含勘误的内容)或者修订版均不适合于本标准,但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 17859—1999 计算机信息系统安全保护等级划分准则

GB/T 5271.8—2001 信息系统 词汇 第8部分:安全(idt ISO/IEC 2382-8:1998)

GB/T 18336(所有部分) 信息技术 安全技术 信息技术安全性评估准则(GB/T 18336—2001, idt ISO/IEC 15408:1999)

3 术语和定义及记法

GB 17859—1999、GB/T 5271.8—2001 和 GB/T 18336—2001 确立的及以下术语和定义适用于本标准。

3.1 术语和定义

3.1.1

安全审计 security audit

对信息系统的各种事件及行为实行监测、信息采集、分析并针对特定事件及行为采取相应比较动作。

3.1.2

事件辨别器 event discriminator

提供事件最初的识别并决定是否向审计记录器传送该事件消息和产生审计报警的功能部件。

3.1.3

审计记录器 audit recorder

产生审计记录并将记录保存在本地或远程系统的功能部件。

3.1.4

审计分析器 audit analyzer

检查审计记录,以确认是否需要产生审计报警及采取相应行动的功能部件,对分析结果进行数据汇总,发送至报表生成器。

3.1.5

报表生成器 report processor

根据数据分析结论,进行报告处理,生成相关报告的功能部件。

3.1.6

报警处理器 alarm processor

接受审计报警请求并产生响应动作的功能部件。

3.1.7

审计踪迹审阅器 audit trail examiner

用来检阅审计记录并产生分析报告的功能部件。

3.1.8

审计备份器 audit archiver

根据授权管理员的要求将审计记录的全部或部分备份到安全存储介质的功能部件。

3.1.9

审计代理 audit agent

安全审计系统中完成审计数据采集、鉴别并向审计跟踪记录中心发送审计消息的功能部件，包括软件代理和硬件代理。

3.1.10

审计跟踪记录中心 audit trail center

安全审计系统中负责接收各审计代理发送的审计消息并对消息进行记录、分析、报警、生成报告和备份的功能部件。

3.1.11

授权管理员 authorized administrator

可管理安全审计产品组件的授权用户。

3.1.12

嗅探 sniffing

对网络线路上传送的数据包进行捕获以获得信息的行为。

3.1.13

入侵 intrusion

任何企图危害资源保密性、完整性或可用性的行为。

3.2 记法

本标准中所用记法，采用了以下两种标识：

a) 采用符号【】内加文字表示，区别不同类别的产品要求。用【专用型】和【综合型】表示安全审计产品的2个类别。未标注【专用型】或【综合型】的要求及方法适用于全部安全审计产品；

b) 本标准对安全审计产品进行了分级。本标准中的规定，凡未特殊说明，均为基本型产品要求，对于增强型产品的要求，采用内容以黑体字加以标识。

4 安全审计产品分类

4.1 专用型

对主机、服务器、网络、数据库管理系统、其他应用系统等客体采集对象其中一类进行审计，并对审计事件进行分析和响应的安全审计产品。

4.2 综合型

对主机、服务器、网络、数据库管理系统、其他应用系统中至少两类客体采集对象进行审计，并对审计事件进行统一分析与响应的安全审计产品。

5 安全功能要求

5.1 审计踪迹

5.1.1 审计事件生成

5.1.1.1 审计数据采集

【专用型】产品应包括以下一类采集范围，【综合型】产品至少应包括以下两类采集范围：

a) 主机、服务器审计数据采集：

1) 目标主机的启动和关闭；

2) 目标主机操作系统的日志；

3) 目标主机的软、硬件等配置信息；

4) 目标主机网络连接；

5) 目标主机的外围设备使用；

6) 目标主机的文件使用。

b) 网络审计数据采集：

1) 网络协议；

2) 网络流量；

3) 入侵行为。

c) 数据库管理系统审计数据采集：

1) 数据库数据操作；

2) 数据库结构操作；

3) 数据库用户更改。

d) 其他应用系统审计数据采集：

1) 目标应用系统日志；

2) 目标应用系统操作。

5.1.1.2 紧急事件报警

对于系统安全策略定义的紧急事件，产品应直接向报警处理器发送报警消息，并记录报警数据。

5.1.1.3 审计数据生成

产品应在实际的系统环境和网络带宽下及时的进行审计数据生成。

5.1.1.4 事件辨别扩展接口

产品应提供一个功能接口，对其自身无法辨别的安全事件，用户可通过该接口，将扩展的事件辨别模块以插件的形式接入事件辨别器。

5.1.2 审计记录

5.1.2.1 记录内容

产品应按照事件的分类和级别，生成包含以下内容的审计记录：

a) 事件 ID；

b) 事件主体；

c) 事件客体；

d) 事件发生的日期和时间；

e) 事件类型；

f) 事件的级别；

g) 审计源身份；

h) 事件的结果(成功或失败)。

5.1.2.2 数据库支持

产品应支持至少一种数据库管理软件，将审计记录存放到数据库中，方便用户查阅、检索和统计分析。

5.1.2.3 **数据安全存储**

产品应对产生的审计记录数据进行保护，防止其被泄漏、篡改和丢失。

5.1.3 **审计统计分析**

5.1.3.1 **审计统计**

产品应对审计事件的发生总数、单个审计事件累计发生次数或单个审计事件发生频率进行数值统计，并对不规则或频繁出现的事件进行概率统计。

5.1.3.2 **潜在危害**

产品应提供一个审计事件集合。当这些事件的累计发生次数或发生频率超过设定的阈值时，表明信息系统出现了可能的潜在危害。针对这些事件集合，应有一个固定的规则集，利用该规则集对信息系统的潜在危害进行分析。审计事件集合应可定制。

5.1.3.3 **异常事件和行为**

产品应维护一个与信息系统相关的异常事件集合。当这些异常事件发生时表明信息系统受到了攻击。异常事件集合应可定制。

产品至少应对下列异常事件和行为进行分析处理：

a) 用户活动异常；

b) 系统资源滥用或耗尽；

c) 网络应用服务超负荷；

d) 网络通信连接数剧增。

5.1.3.4 **关联行为**

产品应对关联行为进行以下操作：

a) 对相互关联的事件进行综合分析和判断；

b) 向授权用户提供自定义匹配模式；

c) 【综合型】产品应能进行多审计类型关联分析。

5.1.3.5 **审计分析接口**

产品应提供审计分析接口，由用户选择不同的审计分析模块以增强自身的审计分析能力。

5.1.3.6 **系统报警记录**

当审计分析器的分析表明信息系统出现潜在危害、异常事件以及攻击行为时，产品报警处理器应生成报警记录。报警记录应包括下列内容：

a) 事件 ID；

b) 事件主体；

c) 事件客体；

d) 事件发生时间；

e) 事件危险级别；

f) 事件描述；

g) 事件结果(成功或失败)。

5.1.3.7 **审计分析报表**

报表生成器将审计分析器传来的分析结果进行数据汇总报表输出，对报表至少有以下要求：

a) 产品应至少支持按关键字生成、按模块功能生成、按危害等级生成、按自定义格式生成等分析报表生成方式；

b) 报表内容应至少支持文字、图像两种描述方式；

c) 审计数据报表生成格式应至少支持 txt、html、doc、xls 等通用文件格式中的一种。

5.1.4 **事件响应**

产品应对事件辨别器和审计分析器发送的报警记录采取相应的响应动作。

5.1.4.1 响应报警

产品应产生响应报警。响应报警方式至少包含以下方式中的两种：

a) 向系统管理员发送报警邮件；

b) 向网管中心发送 SNMP、Trap 报警消息；

c) 向声光电报警装置发送启动信号；

d) 向网管人员发送 SMS 报警短消息。

5.1.4.2 响应措施

产品应采取相应响应措施，以保证信息系统以及自身的安全。应采取下列至少一种形式的响应方式：

a) 对策略中标记为阻断的攻击进行阻断；

b) 调用授权管理员预定义的操作或应用程序；

c) 与其他网络产品进行联动。

5.1.4.3 联动

a) 产品应与其他类型的安全产品以相互确认的协议或通讯方式交流审计信息，采取联合行动以加固或保护被审计信息系统。

b) 产品应至少提供一个标准的、开放的接口，能按照该接口规范为其他类型安全产品编写相应的程序模块，达到与其联动的目的。

5.1.5 审计查阅

5.1.5.1 常规查阅

产品应提供查阅审计记录的工具，查阅的结果应以用户易于理解的方式和格式提供，并且能生成报告和进行打印。

5.1.5.2 有限查阅

产品应确保除授权管理员之外，其他用户无权对审计记录进行查阅。

5.1.5.3 可选查阅

产品应为授权管理员提供将审计记录按一定的条件进行选择、搜索、分类和排序的功能，所得结果应以用户友好的、便于理解的形式提供报告或打印。

5.1.6 审计记录存储

5.1.6.1 安全保护

产品应至少采取一种安全机制，保护审计记录数据免遭未经授权的删除或修改，如采取严格的身份鉴别机制和适合的文件读写权限等。任何对审计记录数据的删除或修改都应生成系统自身安全审计记录。

5.1.6.2 可用性

在审计存储空间耗尽、遭受攻击等异常情况下，产品应采取相应措施保证已存储的审计记录数据的可用性。

5.1.6.3 保存时限

产品应提供设置审计记录保存时限的最低值功能，用户可根据自身需要设定记录保存时间。

5.1.7 审计策略

5.1.7.1 事件分类和分级

产品应对可审计跟踪的事件按用户可理解的方式进行分类，方便用户浏览和策略定制。同时应将可审计事件的重要程度划分为不同的级别，对不同级别的事件采取不同的处理方式。

5.1.7.2 缺省策略

产品应设置系统缺省策略，对可审计事件进行审计。

5.1.7.3 策略模板

产品应为用户提供多套策略模板，使用户可根据具体的信息系统要求选择最适宜的审计策略，对可审计事件进行审计。

5.1.7.4 策略定制

产品应为用户提供可自主定制的审计策略定制功能。

5.2 审计数据保护

5.2.1 数据传输控制

审计代理与审计跟踪记录中心相互传输审计记录数据及配置和控制信息时，产品应确保只有授权管理员能启动或停止数据传输。

5.2.2 数据传输安全

产品在审计代理与审计跟踪记录中心相互传输审计记录数据及配置和控制信息时，传输数据应加密，并采取措施保证数据完整。

5.3 安全管理

5.3.1 管理角色

产品应为管理角色进行分级，使不同级别的管理角色具有不同的管理权限。

5.3.2 操作审计

产品应对不同管理角色在管理期间的全部活动生成相应的审计记录。

5.3.3 安全状态监测

管理员应能实时监测产品的运行情况，并对其产生的日志和报警信息进行汇总和统一分析。

5.4 标识和鉴别

5.4.1 管理角色属性

产品应为每个管理角色规定与之相关的安全属性，如管理角色标识、鉴别信息、隶属组、权限等，并提供使用默认值对创建的每个管理角色的属性进行初始化的功能。

5.4.2 身份鉴别

5.4.2.1 用户鉴别

在任何用户需要执行管理功能之前，产品应对该管理角色的身份进行鉴别。

5.4.2.2 多鉴别

产品应能向管理角色提供除口令身份鉴别机制以外的其他身份鉴别机制（如智能IC卡、指纹、视网膜等鉴别机制）。

5.4.2.3 重鉴别

当已通过身份鉴别的管理角色空闲操作的时间超过规定值，在该管理角色需要执行管理功能前，产品应对该管理角色的身份重新进行鉴别。

5.4.3 鉴别数据保护

产品应保证鉴别数据不被未授权查阅或修改。

5.4.4 鉴别失败处理

产品应为管理员登录设定一个授权管理员可修改的鉴别尝试阈值，当管理员的不成功登录尝试超过阈值，系统应通过技术手段阻止管理员的进一步鉴别请求。

5.5 产品升级

5.5.1 手动升级

授权管理员能定期对产品进行手动的升级，如更新匹配规则库、策略文件以及服务程序等。授权管理员取得升级包后，能按照升级说明文件的要求，对系统进行升级。

5.5.2 自动升级

产品应定期检查相关升级网站，自动下载系统升级包，下载完毕后自动运行升级程序进行升级。升级

过程中可暂时终止系统服务程序的运行，升级完成后应重新启动服务程序，按照原有的策略继续运行。

自动升级应采取身份验证、数字签名等手段避免得到错误或伪造的系统升级包。

5.5.3 审计代理升级

分布式审计所包含的各审计代理应支持自动检测审计中心版本，自动下载升级包，进行升级。

5.5.4 升级日志记录

产品应自动审计记录升级日志。升级日志至少应包含时间、版本等信息。

5.6 监管要求

产品可兼具监管功能。部分安全事件可通过使用监管功能进行管理。

6 自身安全要求

6.1 自身审计数据生成

产品应对与自身安全相关的以下事件生成审计记录：

a) 对产品进行操作的尝试，如关闭审计功能或子系统；

b) 产品管理员的登录和退出；

c) 对安全策略进行更改的操作；

d) 读取、修改、破坏审计跟踪数据的尝试；

e) 因鉴别尝试不成功的次数超出了设定的限值，导致的会话连接终止；

f) 对管理角色进行增加，删除和属性修改的操作；

g) 对其他安全功能配置参数的修改(设置和更新)，无论成功与否。

6.2 自身安全审计记录独立存放

产品应将自身安全审计记录与被审计的目标信息系统的审计记录分开保存到不同的记录文件或数据库(或同一数据库的不同表)中，方便用户查阅和分析。

6.3 审计代理安全

a) 由产品提供的软件代理应具备自保护能力，使用专用卸载程序对软件代理进行卸载时应提供密码保护，除专用卸载程序外用户不可手工删除、停用。

b) 审计跟踪记录中心应提供检测信息系统是否已安装软件代理的功能。若未安装软件代理，将产生报警。

6.4 产品卸载安全

卸载产品时，应对产品中保存的审计数据进行删除，或提醒用户删除。进行产品删除操作的用户应该具有相应的权限。

6.5 系统时间同步

产品应提供同步审计代理与审计跟踪记录中心时间的功能，并应同时自动记录审计代理与审计跟踪记录中心的时间。

6.6 管理信息传输安全

安全审计产品需要通过网络进行管理时，安全审计产品应能对管理信息进行保密传输。

6.7 系统部署安全

产品应支持多级分布式部署模式，保证安全审计系统某分中心遭受攻击、通讯异常等问题时产品正常运行。

6.8 审计数据安全

安全审计产品应对本地审计数据保密存储。

7 性能要求

7.1 稳定性

软件代理在宿主操作系统上应工作稳定，不应造成宿主机崩溃情况。

硬件代理产品在与产品设计相适应的网络带宽下应运行稳定。

7.2 资源占用

软件代理的运行对宿主机资源(如CPU、内存空间和存储空间),不应长时间固定或无限制占用,不应影响对宿主机合法的用户登录和资源访问。

7.3 网络影响

产品的运行不应对原网络正常通讯产生长时间固定影响。

7.4 吞吐量

产品应有足够的吞吐量,保证对被审计信息系统接受和发送的海量数据的控制。在大流量的情况下,产品应通过自身调节做到动态负载均衡。

8 保证要求

8.1 配置管理保证

8.1.1 开发商应使用配置管理系统并提供配置管理文档,为产品的不同版本提供唯一的标识。

8.1.2 配置管理系统应对所有的配置项作出唯一的标识,并保证只有经过授权才能修改配置项。

8.1.3 配置管理文档应包括配置清单和配置管理计划。在配置清单中,应对每一配置项给出相应的描述;在配置管理计划中,应描述配置管理系统是如何使用的。实施的配置管理应与配置管理计划相一致。

8.1.4 配置管理文档还应描述对配置项给出唯一标识的方法,并提供所有的配置项得到有效地维护的证据。

8.1.5 开发者应提供配置管理文档。配置管理文档应说明配置管理系统至少能跟踪:安全审计产品实现表示、设计文档、测试文档、用户文档、管理员文档和配置管理文档,并描述配置管理系统是如何跟踪配置项的。

8.2 交付与运行保证

8.2.1 开发者应使用一定的交付程序交付安全审计产品,并将交付过程文档化。

8.2.2 交付文档应描述在给用户方交付协议安全审计产品的各版本时,为维护安全所必需的所有程序。

8.2.3 开发者应提供文档说明协议安全审计产品的安装、生成、启动和日志生成的过程。

8.3 指导性文档

8.3.1 管理员指南

a) 开发商应提供针对产品管理员的管理员指南。

b) 管理员指南应描述管理员可使用的管理功能和接口。

c) 管理员指南应描述怎样以安全的方式管理产品。

d) 对于在安全处理环境中必须进行控制的功能和特权,管理员指南应提出相应的警告。

e) 管理员指南应描述所有对与安全审计产品的安全操作有关的用户行为的假设。

f) 管理员指南应包含安全功能如何相互作用的指导。

g) 每一种与管理功能有关的安全相关事件,包括对安全功能所控制的实体的安全特性进行的改变。

h) 所有与系统管理员有关的IT环境的安全要求。

i) 管理员指南应与为评价而提供的其他所有文件保持一致。

8.3.2 用户指南

a) 开发商应提供用户指南。

b) 用户指南应描述非管理员用户可用的功能和接口。

c) 用户指南应包含使用产品提供的安全功能和指导。

d) 用户指南应描述用户可获取但应受安全处理环境控制的所有功能和权限。

e) 用户指南应清晰地阐述产品安全运行中用户所必须负的职责，包含产品在安全使用环境中对用户行为的假设。

f) 用户指南应描述与用户有关的 IT 环境的所有安全要求。

g) 用户指南应与为评价而提供的其他所有文件保持一致。

8.4 测试保证

8.4.1 功能测试

a) 开发商应测试产品的功能，并记录结果。

b) 开发商在提供产品时应同时提供该产品的测试文档。

c) 测试文档应由测试计划、测试过程描述、预期的测试结果和实际测试结果组成。

d) 测试文档应标识将要测试的产品功能，并描述将要达到的测试目标。

e) 测试过程应标识要执行的测试，并描述每个安全功能的测试概况，这些概况包括对其他测试结果的顺序依赖性。

f) 开发商的期望测试结果应表明测试成功后的预期输出。实际测试结果应表明每个被测试的安全功能能按照规定进行运作。

8.4.2 测试覆盖面分析报告

a) 开发商应提供对产品测试覆盖范围的分析报告。

b) 测试覆盖面分析报告应证明测试文件中确定的测试项目可覆盖产品的所有安全功能。

8.4.3 测试深度分析报告

a) 开发商应提供对产品的测试深度的分析报告。

b) 测试深度分析报告应证明测试文件中确定的测试能充分表明产品的运行符合安全功能规范。

8.4.4 独立性测试

开发商应提供用于适合测试的部件，且提供的测试集合应与其自测产品功能时使用的测试集合相一致。

8.5 脆弱性分析保证

8.5.1 指南检查

a) 开发者应提供指南性文档。

b) 在指南性文档中，应确定对产品的所有可能的操作方式(包含失败和操作失误后的操作)、它们的后果以及对于保持安全操作的意义。指南性文档中还应列出所有目标环境的假设以及所有外部安全措施(包含外部程序的、物理的或人员的控制)的要求。指南性文档应是完整的、清晰的、一致的、合理的。

8.5.2 脆弱性分析

a) 开发者应从用户可能破坏安全策略的明显途径出发，对产品的各种功能进行分析并提供文档。对被确定的脆弱性，开发者应明确记录采取的措施。

b) 对每一条脆弱性，应有证据显示在使用产品的环境中该脆弱性不能被利用。在文档中，还需证明经过标识脆弱性的产品可以抵御明显的穿透性攻击。

c) 脆弱性分析文档应明确指出产品已知的安全隐患、能够侵犯产品的已知方法以及如何避免这些隐患被利用。

8.6 生命周期支持

a) 开发者应提供开发安全文件。

b) 开发安全文件应描述在产品的开发环境中，为保护产品设计和实现的机密性和完整性，而在物理上、程序上、人员上以及其他方面所采取的必要的安全措施。开发安全文件还应提供在产

品的开发和维护过程中执行安全措施的证据。

9 测评方法

9.1 安全功能

9.1.1 审计跟踪

9.1.1.1 审计事件生成

9.1.1.1.1 审计数据采集

a) 评价内容：见 5.1.1.1。

b) 测试评价方法：

1) 主机、服务器审计测试：

——启动和关闭目标主机，审查审计记录；

——审查目标主机的操作系统日志审计记录；

——审查目标主机的软、硬件信息审计记录；

——从目标主机进行网络连接，审查审计记录。

——模拟使用目标主机的外围设备，审查审计记录；

——模拟使用目标主机文件，审查审计记录。

2) 网络审计测试：

——从目标主机发起服务请求，审查协议审计记录；

——向网络上发送大量畸形数据包造成网络流量加大，审查审计记录；

——模拟网络入侵行为，进行审计记录。

3) 数据库管理系统审计测试：

——模拟进行数据库数据操作，审查审计记录；

——模拟更改数据库结构，审查审计记录；

——模拟更改数据库用户，审查审计记录。

4) 其他应用系统审计测试：

——审查目标应用系统日志审计记录；

——进行目标应用系统操作，审查审计记录。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1) 【专用型】符合以上四项其中一项测试要求，【综合型】至少符合其中两项测试要求。

2) 对每一个测试都产生正确的审计记录。

3) 产生的审计记录与事件存在明确的对应关系。

9.1.1.1.2 紧急事件报警

a) 评价内容：见 5.1.1.2。

b) 测试评价方法：

1) 检查系统配置是否支持紧急事件定义；

2) 生成紧急事件；

3) 检查审计记录；

4) 检查报警处理器是否采取了相应的响应措施。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1) 系统配置应支持紧急事件定义；

2) 审计记录应能准确记录紧急事件；

3) 报警处理器应能采取响应措施。

9.1.1.1.3 审计数据生成

a) 评价内容：见 5.1.1.3。

b) 测试评价方法：

1) 将产品部署在测试环境；

2) 按照用户要求，进行安全审计数据及时收集；

3) 检查审计跟踪检验器。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断。审计数据应能实时生成。

9.1.1.1.4 事件辨别扩展接口

a) 评价内容：见 5.1.1.4。

b) 测试评价方法：

1) 检查事件定义模块；

2) 自定义安全事件模块。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1) 产品支持自定义的安全事件；

2) 产品能检测自定义的安全事件。

9.1.1.2 审计记录

9.1.1.2.1 记录内容

a) 评价内容：见 5.1.2.1。

b) 测试评价方法：评价者应审查审计记录中是否包含 5.1.2.1 中规定的内容。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，审计记录应详细、完整、容易理解。

9.1.1.2.2 数据库支持

a) 评价内容：见 5.1.2.2。

b) 测试评价方法：评价者应审查产品支持的数据库类型。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断。产品应支持产品说明手册声称支持的数据库类型，支持的数据库类型至少包含一种数据库管理软件，如 SQL Server、Oracle 等。

9.1.1.2.3 数据安全存储

a) 评价内容：见 5.1.2.3。

b) 测试评价方法：

1) 评价者应审查产品说明手册声称的审计记录安全措施；

2) 对声称的措施进行核实。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断。产品应对产生的审计记录数据进行保护。

9.1.1.3 审计统计分析

9.1.1.3.1 审计统计

a) 评价内容：见 5.1.3.1 的内容。

b) 测试评价方法：

1) 评价者应检查审计事件统计实现方法；

2) 评价者应模拟产生相应的审计事件。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1) 审计事件统计类型正确；

2） 审计事件统计结果正确。

9.1.1.3.2 潜在危害

a） 评价内容：见 5.1.3.2。

b） 测试评价方法：

1） 评价者应检查审计事件集合；

2） 评价者应检查事件报警触发条件。

c） 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1） 审计事件集合分类清晰；

2） 事件报警触发条件合理；

3） 审计事件及报警触发条件可订制。

9.1.1.3.3 异常事件和行为

a） 评价内容：见 5.1.3.3。

b） 测试评价方法：

1） 用户越权访问，审查审计记录；

2） 耗尽系统资源，审查审计记录；

3） 网络应用服务超负荷，审查审计记录；

4） 建立大量网络通信连接，审查审计记录。

c） 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1） 对每一个测试产生正确的审计记录；

2） 产生的审计记录与事件存在明确的对应关系。

9.1.1.3.4 关联行为

a） 评价内容：见 5.1.3.4。

b） 测试评价方法：

——评价者应审查产品手册产品是否具有关联分析能力并验证；

——评价者应审查产品手册产品是否提供自定义匹配模式并验证；

——评价者应审查多审计类型关联分析的能力。

c） 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

——产品对相互关联的事件能利用关联分析相关技术进行综合分析和判断；

——产品能向授权用户提供自定义匹配模式；

——产品可进行关联分析形成最终报表。

9.1.1.3.5 审计分析接口

a） 评价内容：见 5.1.3.5。

b） 测试评价方法：

1） 查看产品说明手册是否包含提供审计分析接口的说明；

2） 对审计分析接口进行测试，是否可选择不同的审计分析模块。

c） 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1） 产品应提供审计分析接口；

2） 审计分析接口设计灵活，使用户可选择不同的审计分析模块。

9.1.1.3.6 审计报警记录

a） 评价内容：见 5.1.3.6。

b） 测试评价方法：

1） 评价者应审查产品的报警信息是否详细、完整、容易理解；

2） 评价者应审查产品的报警信息是否包含 5.1.3.6 中规定的内容：事件 ID、事件主体、事件

客体、事件发生时间、事件危险级别及事件描述。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，评价者审查内容应包含以上两方面。

9.1.1.3.7 审计分析报表

a) 评价内容：见5.1.3.7。

b) 测试评价方法：

1) 模拟生成产品报表，检查产品的生成报表是否详细、完整、容易理解；

2) 评价者应审查产品是否能支持按关键字生成、按模块功能生成、按危害等级生成、按自定义格式生成等方式生成审计分析报表；

3) 评价者应审查产品是否能支持文字、图像两种描述方式；

4) 评价者应审查审计数据报表是否能支持txt、html、doc、xls等通用文件格式。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，评价者审查内容应包含以上四方面。

9.1.1.4 事件响应

9.1.1.4.1 响应报警

a) 评价内容：见5.1.4.1。

b) 测试评价方法：

1) 评价者应审查产品说明手册对支持响应报警方式的描述；

2) 验证响应报警方式是否准确、有效。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1) 产品提供至少两种响应报警方式；

2) 响应报警方式准确、有效。

9.1.1.4.2 响应措施

a) 评价内容：见5.1.4.2。

b) 测试评价方法：评价者应审查产品说明手册是否包含产品对支持的响应方式的描述，并且测试响应机制是否准确、有效。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断。

9.1.1.4.3 联动

a) 评价内容：见5.1.4.3。

b) 测试评价方法：

1) 评价者应审查产品说明书是否描述产品支持与其他产品的联动；

2) 按照产品说明书，测试产品是否可与其他产品联动；

3) 评价者应审查产品说明书是否描述产品提供联动接口。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1) 产品支持与其他产品的联动；

2) 产品为与其他产品的联动提供相应设置；

3) 产品应提供公开的联动接口。

9.1.1.5 审计查阅

9.1.1.5.1 常规查阅

a) 评价内容：见5.1.5.1。

b) 测试评价方法：

1) 打开审计跟踪审阅器；

2) 查阅审计记录，生成报告，打印报告。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1) 提供审计查阅功能；

2) 审计查阅以用户易理解的方式和格式提供；

3) 提供生成报告并打印的功能。

9.1.1.5.2 **有限查阅**

a) 评价内容：见 5.1.5.2。

b) 测试评价方法：

1) 评价者以不具有审计查阅权限的用户身份登录系统；

2) 查阅审计记录，生成报告，打印报告；

3) 进入审计记录存储的目录，检查是否可以查看审计记录。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1) 只有经过授权的用户能查阅审计记录；

2) 审计记录以不可理解的格式进行存储。

9.1.1.5.3 **可选查阅**

a) 评价内容：见 5.1.5.3。

b) 测试评价方法：

1) 进入审计跟踪审阅器；

2) 进行选择、搜索、分类、排序操作。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1) 具有针对审计记录选择、搜索、分类、排序的能力；

2) 处理时具有友好的用户界面，提供便于理解的处理结果。

9.1.1.6 **审计记录存储**

9.1.1.6.1 **安全保护**

a) 评价内容：见 5.1.6.1。

b) 测试评价方法：

1) 评价者应审查产品说明手册是否包含对审计记录保护机制的描述；

2) 对保护机制进行核实；

3) 对审计记录数据进行删除或修改。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1) 产品具有有效机制保护审计记录免遭未授权的删除或修改；

2) 针对审计记录数据的删除或修改生成系统自身安全审计记录。

9.1.1.6.2 **可用性**

a) 评价内容：见 5.1.6.2。

b) 测试评价方法：

1) 评价者应审查产品说明手册具有何种保证审计记录可用性的机制；

2) 对保证机制进行核实。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1) 产品崩溃时审计记录的丢失控制在可接受的程度；

2) 产品能向用户提供可选择操作以处理审计记录存储空间满的问题，如回滚等；

3) 用户可定制警戒值，当审计记录存储空间达到警戒值时，触发报警机制。

9.1.1.6.3 **保存时限**

a) 评价内容：见 5.1.6.3。

b) 测试评价方法：

1） 评价者应审查产品说明手册中审计数据最低保存时限的说明；

2） 对产品是否允许用户设置保存时限进行核实。

c） 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断。产品应具有为审计数据设置最低保存时限的功能。

9.1.1.7 审计策略

9.1.1.7.1 事件分级和分类

a） 评价内容：见5.1.7.1。

b） 测试评价方法：

1） 打开审计跟踪审阅器；

2） 查看是否对可审计事件进行分类、分级。

c） 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应满足：

1） 对可审计事件进行分类和分级；

2） 事件分类采用用户可理解的、主流的分类方法；

3） 事件分级有明确界定范围。

9.1.1.7.2 缺省策略

a） 评价内容：见5.1.7.2。

b） 测试评价方法：

1） 打开审计跟踪审阅器；

2） 查看产品是否具有缺省策略；

3） 对缺省策略进行核实验证。

c） 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1） 产品具有缺省策略；

2） 产品能按照缺省策略对可审计事件进行审计。

9.1.1.7.3 策略模板

a） 评价内容：见5.1.7.3。

b） 测试评价方法：打开审计跟踪审阅器，检查产品是否提供两套以上的策略模板。

c） 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1） 产品应具有两套以上的缺省策略；

2） 内置策略应有明显区别，适用于不同审计环境。

9.1.1.7.4 策略定制

a） 评价内容：见5.1.7.4。

b） 测试评价方法：打开审计跟踪审阅器，检查产品是否提供策略定制能力。

c） 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1） 产品提供策略定制功能；

2） 策略定制提供向导功能，能进行复杂条件的定制。

9.1.2 审计数据保护

9.1.2.1 数据传输控制

a） 评价内容：见5.2.1。

b） 测试评价方法：评价者分别以授权管理员和非授权管理员的身份登录系统，在审计代理和审计跟踪记录中心间传输审计记录数据及配置和控制信息。

c） 测试评估结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1） 授权管理员可进行数据传输，可决定数据传输的启动或终止；

2） 非授权管理员不能进行数据传输。

9.1.2.2 数据传输安全

a) 评价内容：见 5.2.2。

b) 测试评价方法：

1) 在审计代理和审计跟踪记录中心之间传递信息，通过网络嗅探的方式获取传输的内容；

2) 通过网络注入的方式篡改传输的数据，审查系统是否能够发现；

3) 人为制造异常中断，审查重新连接后是否重传；

4) 审查开发者文档中对保证审计代理和审计跟踪记录中心之间传递信息的安全性的描述。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1) 获取的内容应为不可理解的内容；

2) 传输数据被篡改后，系统提示异常或重新传输；

3) 重新连接后，系统能重发数据；

4) 开发者文档提供为保证审计代理和审计跟踪记录中心之间数据传输安全性所采取措施的详细描述，列举所采取的措施。

9.1.3 安全管理

9.1.3.1 管理角色

a) 评价内容：见 5.3.1。

b) 测试评价方法：

1) 检查产品是否允许定义多个角色；

2) 检查产品是否具有多种管理角色权限；

3) 检查各角色是否可以进行权限划分。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1) 可把用户定义为多个角色；

2) 系统管理员、日志查看员、审计日志查看员三种管理角色权限分开；

3) 每个角色可具有多个用户，每个用户只属于一个角色；

4) 每一个用户标识是全局唯一的，不应一个用户标识用于多个用户。

9.1.3.2 操作审计

a) 评价内容：见 5.3.2。

b) 测试评价方法：

1) 评价者应审查产品说明书是否详细描述系统所支持的审计行为；

2) 评价者应切换不同角色对系统进行操作测试并查看审计记录是否对不同角色的管理行为进行详细而正确的记录。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，评价者审查内容应包含以上三方面。

9.1.3.3 安全状态监测

a) 评价内容：见 5.3.3。

b) 测试评价方法：

1) 查询产品说明书，查看系统是否支持管理员安全状态监测功能；

2) 以授权管理员角色登录系统，进行产品状态监测，模拟状态变化日志和报警，测试日志和报警信息汇总和统一分析功能。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1) 产品说明书应详细描述支持的安全状态监测功能；

2) 管理员应可以实时对系统进行安全状态监测。

9.1.4 标识和鉴别

9.1.4.1 管理角色属性

a) 评价内容：见 5.4.1。

b) 测试评价方法：

1) 评价者应审查产品说明手册中是否为各管理角色规定与之相关的安全属性，如管理角色标识、鉴别信息、隶属组、权限等；

2) 分别以不同管理角色身份登录，测试产品是否使用默认值对创建的各管理角色的属性进行初始化。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1) 产品说明手册为各管理角色规定与之相关的安全属性；

2) 产品使用默认值对创建的各管理角色的属性进行初始化。

9.1.4.2 身份鉴别

9.1.4.2.1 用户鉴别

a) 评价内容：见 5.4.2.1。

b) 测试评价方法：登录产品，并切换为不同用户，检查是否在执行管理功能之前要求首先进行身份认证。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1) 在用户执行管理功能之前对用户进行身份鉴别；

2) 登录之前可执行操作仅有输入登录信息、查看登录帮助；

3) 用户没有切换角色而执行本角色具有权限的管理功能时，不必重新认证。

9.1.4.2.2 多鉴别

a) 评价内容：见 5.4.2.2。

b) 测试评价方法：用不同角色登录产品，检查产品是否支持对高级别用户的高强度鉴别机制。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1) 产品至少提供两种鉴别机制；

2) 对于高级别用户，产品提供更高强度的鉴别机制。

9.1.4.2.3 重鉴别

a) 评价内容：见 5.4.2.3。

b) 测试评价方法：

1) 审查产品说明书是否描述产品支持重鉴别，并获取空闲操作的阈值；

2) 登录产品并空闲操作达到阈值，然后执行管理功能，检查产品是否要求重新鉴别。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1) 产品说明书详细说明重鉴别的阈值及设置方法；

2) 登录产品后并空闲时间超过阈值后，执行管理功能时，产品要求用户重新鉴别。

9.1.4.3 鉴别数据保护

a) 评价内容：见 5.4.3。

b) 测试评价方法：模拟非授权用户查阅或修改鉴别数据。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，产品应只允许授权用户查阅或修改鉴别数据。

9.1.4.4 鉴别失败处理

a) 评价内容：见 5.4.4。

b) 测试评价方法：

1) 检查产品是否定义用户鉴别尝试的最大允许失败次数；

2） 检查产品是否定义当用户连续鉴别尝试失败达到阈值后采取的措施；

3） 尝试多次失败的用户鉴别行为，检查达到阈值后，系统是否采取相应措施并生成审计事件。

c） 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1） 产品具备定义用户鉴别尝试的最大允许失败次数的功能；

2） 产品定义了当用户鉴别尝试失败连续达到指定次数后采取的措施；

3） 当用户连续鉴别尝试失败达到阈值后，产品实施措施并将有关信息生成审计事件；

4） 最大允许失败次数仅由授权管理员设定；

5） 解除措施的权限仅超级管理员具有。

9.1.5 产品升级

9.1.5.1 手动升级

a） 评价内容：见5.5.1。

b） 测试评价方法：

1） 审查产品说明书是否描述产品支持手动升级；

2） 按照产品说明书，测试产品是否可实施手动升级。

c） 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，产品应提供手动升级功能。

9.1.5.2 自动升级

a） 评价内容：见5.5.2。

b） 测试评价方法：

1） 评价者应审查产品说明书是否描述产品支持自动升级；

2） 按照产品说明书，测试产品是否可实施自动升级。

c） 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1） 产品支持自动升级功能；

2） 产品自动升级功能可对升级周期、是否提示用户、是否自动重新启动等进行设置；

3） 产品能对升级包进行校验，防止升级包被篡改或替换。

9.1.5.3 审计代理升级

a） 评价内容：见5.5.3。

b） 测试评价方法：

1） 评价者应审查产品说明书是否描述产品支持审计代理升级；

2） 按照产品说明书，测试审计代理是否可检测中心版本，下载相应升级包，实施在线升级。

c） 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1） 产品支持审计代理升级功能；

2） 审计代理可检测中心版本，下载相应升级包，进行在线升级。

9.1.5.4 升级日志记录

a） 评价内容：见5.5.4。

b） 测试评价方法：

1） 评价者应审查产品是否可自动审计记录升级日志；

2） 评价者应审查升级日志是否包含时间、版本等信息。

c） 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1） 产品可自动审计记录升级日志；

2） 升级日志包含时间、版本等信息。

9.1.6 监管功能

a) 评价内容：见5.6。

b) 测试评价方法：

1) 评价者应审查产品说明书，产品是否支持对安全事件的监管功能；

2) 测试产品是否可以完成监管操作。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1) 产品说明书描述产品可如何完成监管功能及详细操作过程；

2) 可通过产品完成对安全事件的监管。

9.2 自身安全

9.2.1 自身审计数据生成

a) 评价内容：见6.1。

b) 测试评价方法：

1) 关闭或开启审计功能，审查审计记录；

2) 登录并从产品退出，审查审计记录；

3) 更改产品配置策略，审查审计记录；

4) 读取并尝试修改审计跟踪数据，审查审计记录；

5) 多次尝试不成功的登录产品，审查审计记录；

6) 进行用户管理操作，审查审计记录；

7) 更改安全配置，审查审计记录。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1) 对每一个测试产生正确的审计记录；

2) 产生的审计记录与事件存在明确的对应关系。

9.2.2 自身安全审计记录独立存放

a) 评价内容：见6.2。

b) 测试评价方法：

1) 评价者应审查产品是否生成自身审计记录；

2) 评价者应审查产品自身审计记录是否与其他记录分开保存到不同的记录文件或数据库(或同一数据库的不同表)中。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，评价者审查内容应包含以上两方面。产品自身审计记录应与其他审计记录分开保存。

9.2.3 审计代理安全

a) 评价内容：见6.3。

b) 测试评价方法：

1) 评价者应使用专用卸载程序卸载软件代理，查看是否启动密码保护；

2) 不通过专用卸载程序，测试是否可以删除或停用软件代理；

3) 查看审计跟踪记录中心是否可以检测信息系统软件代理的安装。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1) 具备自保护能力，使用专用卸载程序卸载时密码保护功能启动；

2) 除专用卸载程序外用户不可手工删除、停用软件代理；

3) 审计跟踪记录中心可以检测到信息系统是否安装软件代理，没有安装软件代理则产生报警。

9.2.4 产品卸载安全

a) 评价内容：见6.4。

b) 测试评价方法：评价者应测试在卸载产品时审计数据是否删除或提醒用户删除。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断。卸载产品时，会将产品中保存的审计数据进行删除，或提醒用户删除。

9.2.5 系统时间同步

a) 评价内容：见 6.5。

b) 测试评价方法：

1) 评价者应审查产品说明手册，产品是否提供同步审计代理与审计跟踪记录中心时间的功能；

2) 审查审计代理与审计跟踪记录中心，是否时间同步并有自动记录。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1) 产品提供同步审计代理与审计跟踪记录中心时间的功能；

2) 产品可同时自动记录审计代理与审计跟踪记录中心的时间。

9.2.6 管理信息传输安全

a) 评价内容：见 6.6。

b) 测试评价方法：评价者应审查产品说明手册，当产品需要通过网络进行管理时，是否能提供对管理信息进行保密传输的功能。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断。当产品需要通过网络进行管理时，产品应能对管理信息进行保密传输。

9.2.7 系统部署安全

a) 评价内容：见 6.7。

b) 测试评价方法：评价者应审查产品说明手册，产品是否支持多级分布式部署模式。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断。产品应支持多级分布式部署模式。

9.2.8 审计数据安全

a) 评价内容：见 6.8。

b) 测试评价方法：评价者应审查产品说明手册，产品是否提供对本地审计数据保密存储。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断。产品应对本地审计数据保密存储。

9.3 产品性能

9.3.1 稳定性

a) 评价内容：见 7.1。

b) 测试评价方法：

1) 软件代理测试：连续运行产品至少三天，检查是否造成宿主机崩溃或异常；

2) 硬件代理测试：制造与产品设计相应的网络流量，检查产品是否可正常工作。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断，应符合：

1) 软件代理产品：工作稳定，不应造成主机崩溃或异常的情况；

2) 硬件代理产品：工作稳定。

9.3.2 资源占用

a) 评价内容：见 7.2。

b) 测试评价方法：对软件代理进行测试，制造大量审计事件后，在宿主机上对资源占用进行检查。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断。在宿主机上的资源占用率应符合送检厂商描述。

9.3.3 网络影响

a) 评价内容：见 7.3。

b) 测试评价方法：对产品进行测试，启动产品前后，对网络流量进行监控。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断。网络流量应符合送检厂商描述。

9.3.4 吞吐量

a) 评价内容：见 7.4。

b) 测试评价方法：向信息系统输送大流量数据，检查信息系统承载情况。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断。产品应能承受网络中大流量数据的传输，达到负载均衡。

9.4 保证要求

9.4.1 配置管理

a) 评价内容：见 8.1。

b) 测试评价方法：评价者应审查开发者所提供的信息是否满足如下要求：

1) 审查产品开发手册，检查开发商是否使用配置管理系统，开发者所使用的版本号与所表示的安全审计产品完全对应，没有歧义。

2) 配置项，要求配置项应有唯一的标识，并保证只有经过授权才能修改配置项。

3) 配置管理文档应包括配置清单、配置管理计划。配置清单用来描述组成安全审计产品的配置项。在配置管理计划中，应描述配置管理系统是如何使用的。实施的配置管理应与配置管理计划相一致。

4) 配置管理文档还应描述对配置项给出唯一标识的方法，并提供所有的配置项得到有效地维护的证据。安全审计产品配置管理范围，要求将安全审计产品的实现表示、设计文档、测试文档、用户文档、管理员文档、配置管理文档等置于配置管理之下，从而确保它们的修改是在一个正确授权的可控方式下进行的，为此要求：

——开发者所提供的配置管理文档应展示配置管理系统至少能跟踪上述配置管理之下的内容。

——文档应描述配置管理系统是如何跟踪这些配置项的。

——文档还应提供足够的信息表明达到所有要求。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断。

9.4.2 交付与运行

a) 评价内容：见 8.2。

b) 测试评价方法：

1) 评价者应审查开发者是否使用一定的交付程序交付安全审计产品，并使用物理文档描述交付过程，并且评价者应审查开发者交付的文档是否包含以下内容：在给用户方交付安全审计产品的各版本时，为维护安全所必需的所有程序；

2) 评价者应审查开发者是否提供了文档说明安全审计产品的安装、生成、启动和使用的过程。用户能够通过此文档了解安装、生成、启动和使用过程。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断。评价者审查内容至少包含测试评价方法中的两方面。

9.4.3 指导性文档

9.4.3.1 管理员指南

a) 评价内容：见 8.3.1。

b) 测试评价方法：评价者应审查开发者是否提供了供系统管理员使用的管理员指南，并且此管

理员指南是否包含如下内容：

1） 描述管理员可使用的管理功能和接口；

2） 描述怎样以安全的方式管理产品；

3） 对于在安全处理环境中必须进行控制的功能和特权，提出相应的警告；

4） 所有对与安全审计产品的安全操作有关的用户行为的假设；

5） 描述所有受管理员控制的安全参数，并给出合适的参数值；

6） 安全功能如何相互作用的指导，安全配置产品的指令；

7） 描述在产品的安全安装过程中可能要使用的所有配置选项，充分描述与安全管理相关的详细过程，指导用户在产品的安装过程中产生安全配置的详细过程。

c） 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断。评价者审查内容至少包含测试评价方法中的七方面。开发者提供的管理员指南应完整，并与为评价而提供的其他所有文件保持一致。

9.4.3.2 用户指南

a） 评价内容：见 8.3.2。

b） 测试评价方法：

1） 评价者应审查开发者是否提供了供系统用户使用的用户指南，并且此用户指南是否包含如下内容：

——描述非管理员用户可用的功能和接口；

——使用产品提供的安全功能和指导；

——用户可获取但应受安全处理环境控制的所有功能和权限；

——清晰阐述产品安全运行中用户必须的职责，包含产品在安全使用环境中对用户行的假设；

——与用户有关的 IT 环境的所有安全要求。

2） 评价者应审查用户指南是否与为评价而提供的其他所有文件保持一致。

c） 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断。评价者审查内容至少包含测试评价方法中的五方面。开发者提供的用户指南应完整，并与为评价而提供的其他所有文件保持一致。

9.4.4 测试保证

9.4.4.1 功能测试

a） 评价内容：见 8.4.1。

b） 测试评价方法：

1） 评价开发者提供的测试文档，是否包含测试计划、测试过程描述和测试结果；

2） 评价测试文档是否标识了将要测试的产品功能，是否描述将要达到的测试目标；

3） 评价测试过程是否标识了要执行的测试，是否描述了每个安全功能的测试概况（这些概况包括对其他测试结果的顺序依赖性）；

4） 评价测试文档的测试结果是否给出全部测试的预期结果；

5） 评价实际测试结果是否表明每个被测试的安全功能能按照规定进行运作。

c） 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断。评价者审查内容至少包含测试评价方法中的五方面。开发者提供的内容应完整。

9.4.4.2 测试覆盖面

a） 评价内容：见 8.4.2。

b） 测试评价方法：评价者应审查开发者提供的测试覆盖分析结果，是否表明测试文件中确定的测试项目与安全功能设计所描述的安全功能是对应的，且可覆盖安全审计产品的所有安全

功能。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断。测试文件中确定的测试项目与安全功能设计所描述的安全功能是对应的，且可覆盖安全审计产品的所有安全功能。

9.4.4.3 测试深度分析

a) 评价内容：见 8.4.3。

b) 测试评价方法：评价者应审查开发商提供的产品测试深度分析结果，是否表明产品的运行符合安全功能规范。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断。测试文件中确定的测试充分表明产品的运行符合安全功能规范。

9.4.4.4 独立性

a) 评价内容：见 8.4.4。

b) 测试评价方法：评价者应审查开发者是否提供了适于测试的产品，且审查测试集是否覆盖开发商自测产品功能时使用的测试集合。

c) 测试评价结果：记录测试结果并对该结果是否符合测试评价方法要求作出判断。开发者提供的产品应能适合第三方测试，且提供的测试集覆盖其自测产品功能时使用的测试集合。

9.4.5 脆弱性分析

9.4.5.1 指南检查

a) 评价内容：见 8.5.1。

b) 测试评价方法：

1) 评价者应确认开发者提供了指南性文档。

2) 评价者应审查开发者提供的指南性文档，是否满足以下要求：

——评价指南性文档，是否确定对产品的所有可能的操作方式（包含失败和操作失误后的操作），是否确定它们的后果，以及是否确定对于保持安全操作的意义；

——评价指南性文档，是否列出所有目标环境的假设以及所有外部安全措施（包含外部程序的、物理的或人员的控制）的要求；

——评价指南性文档是否完整、清晰、一致、合理。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断。开发者提供的评价指南性文档应完整。

9.4.5.2 脆弱性分析

a) 评价内容：见 8.5.2。

b) 测试评价方法：

1) 评价开发者提供的脆弱性分析文档，是否从用户可能破坏安全策略的明显途径出发，对产品的各种功能进行分析；

2) 对被确定的脆弱性，评价开发者是否明确记录采取的措施；

3) 对每一条脆弱性，评价是否有证据显示在使用产品的环境中该脆弱性不能被利用；

4) 评价所提供的文档，是否证明经过标识脆弱性的产品可以抵御明显的穿透性攻击。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断。开发者提供的脆弱性分析文档应完整。

9.4.6 生命周期支持

a) 评价内容：见 8.6。

b) 测试评价方法：评价者应审查开发者所提供的信息是否满足如下要求：

1) 开发人员的安全管理：开发人员的安全规章制度，开发人员的安全教育培训制度和记录；

2) 开发环境的安全管理：开发地点的出入口控制制度和记录，开发环境的温湿度要求和记录，开发环境的防火防盗措施和国家有关部门的许可文件，开发环境中所使用安全产品必须采用符合国家有关规定的产品并提供相应证明材料；

3) 开发设备的安全管理：开发设备的安全管理制度，包括开发主机使用管理和记录，设备的购置、修理、处置的制度和记录，上网管理，计算机病毒管理和记录等；

4) 开发过程和成果的安全管理：对产品代码、文档、样机进行受控管理的制度和记录，若代码和文档进行加密保护必须采用符合国家有关规定的产品并提供相应证明材料。

c) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断。评价者审查内容至少包含测试评价方法中的四方面。开发者提供文档应完整。

附 录 A
（资料性附录）
安全审计流程和跟踪涵盖的阶段

A.1 安全审计流程

信息系统安全审计产品通过软、硬件代理，对客体进行事件采集，将采集到的事件进行事件辨别与分析。若辨别和分析的结果为策略定义的审计记录事件，则信息系统安全审计产品对结果进行汇总处理，如：数据备份和报告生成。若辨别和分析的结果为策略定义的需要响应的事件，则信息系统安全审计产品对结果进行事件响应处理，如：事件报警。同时，信息系统安全审计产品将事件响应产生的结果进行结果汇总，并根据事件响应，调整审计策略，将策略下发到代理，更新代理的事件采集策略。此过程的示意图见图 A.1。

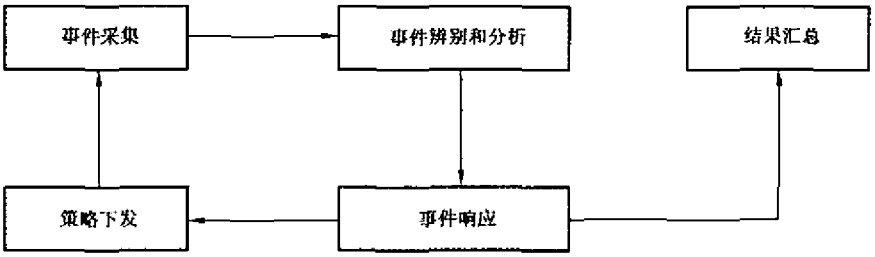

图 A.1 安全审计流程图

A.2 审计跟踪涵盖的阶段

A.2.1 事件采集阶段

a) 事件采集阶段是指审计代理按照预定的审计策略对客体进行相关审计事件采集，并且将形成的结果交由事件处理阶段处理；

b) 对事件处理阶段提交的安全策略分发至各审计代理，审计代理依据安全审计策略对客体进行事件采集。

A.2.2 事件处理阶段

事件处理阶段包含以下行为：

a) 事件处理阶段对采集到的数据进行事件处理，按照预定审计策略进行事件辨析，决定：

1) 忽略该事件；

2) 产生审计信息；

3) 产生审计信息并报警；

4) 产生审计信息且进行响应联动。

b) 对实时信息与审计数据库记录的审计信息，按照用户定义与预定策略进行数据分析并形成审计报告；

c) 对审计记录器按照预定策略进行数据备份；

d) 按照事件响应阶段制定的安全策略，协调各组件的工作。

A.2.3 事件响应阶段

事件响应阶段包含以下行为：

a) 对事件处理阶段产生的报警信息、响应请求进行报警与响应；

b) 对审计分析数据生成各类审计分析报告；

c) 按照预定的安全策略对请求记录与备份数据，写入审计数据库与备份数据库；

d) 根据用户需求制定安全策略并交由事件处理阶段处理。

注：以上各阶段之间并没有必然的时间衔接，它们之间可能存在时间上的间隔或交叉。