ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 911—2010

信息安全技术
日志分析产品安全技术要求

Information security technology—
Security technology requirements for log analysis products

2010-10-30 发布　　2010-11-01 实施

中华人民共和国公安部　发布

目　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由公安部网络安全保卫局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：公安部计算机信息系统安全产品质量监督检验中心。

本标准主要起草人：张笑笑、俞优、吴其聪、邹春明、张艳、顾健。

信息安全技术
日志分析产品安全技术要求

1 范围

本标准规定了日志分析产品的安全功能要求、自身安全功能要求、安全保证要求和等级划分要求。

本标准适用于日志分析产品的设计、开发及检测。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 5271.8—2001 信息技术 词汇 第8部分：安全

GB 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 18336.3—2008 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

3 术语和定义

GB/T 5271.8—2001、GB 17859—1999 和 GB/T 18336.3—2008 界定的以及下列术语和定义适用于本文件。

3.1

日志分析产品 log analysis product

通过日志代理、标准协议、文件导入等方式采集信息系统中的日志数据，并进行集中存储和分析的安全产品。

3.2

日志数据源 log data source

产生日志数据的原始来源。

3.3

日志代理 log agent

完成日志数据采集并向日志管理中心发送采集到的日志数据的功能模块，包括软件代理和硬件代理。

3.4

日志管理中心 log administration center

对采集到的日志数据进行集中处理、存储、分析的功能模块。

3.5

审计日志 audit log

日志分析产品自身审计产生的日志数据。

3.6

日志记录 log record

对采集到的原始日志数据进行预处理之后，根据一定规则生成并保存在日志管理中心的日志数据。

3.7

授权管理员 authorized administrator

具有日志分析产品管理权限的用户，负责对日志分析产品的系统配置、安全策略和日志数据进行管理。

3.8

可信主机 trusted host

赋予权限能够管理日志分析产品的主机。

4 安全功能要求

4.1 日志采集和存储

4.1.1 日志数据源

日志分析产品应能对日志数据源进行添加、修改和删除等管理操作，并且日志数据源的类型应至少包含以下范围：

a) 网络设备，如交换机、路由器、防火墙等；
b) 操作系统；
c) 数据库系统；
d) 其他应用系统。

4.1.2 日志数据采集

4.1.2.1 标准协议接收

日志分析产品应能接收从日志数据源发送的基于 Syslog、Snmp trap、Ftp 或其他标准协议的日志数据。

4.1.2.2 代理方式采集

日志分析产品应能通过日志代理方式采集日志数据源的日志数据。

4.1.2.3 日志文件导入

日志分析产品应能导入通用格式的日志文件。

4.1.2.4 日志采集及时性

日志分析产品应能及时采集日志数据源的日志数据。

4.1.3 日志数据的预处理

4.1.3.1 数据筛选

日志分析产品应能基于既定策略对采集的日志数据进行过滤，有选择地生成日志记录。

4.1.3.2 数据转换

日志分析产品应能将各种不同格式的原始日志数据转换为统一的数据格式，且转换时不能造成关键数据项丢失。

4.1.4 日志记录生成

日志分析产品应在对采集的日志数据进行预处理和事件分析之后，生成相应的日志记录。

日志记录内容应为管理员可理解，并且包含以下信息：

a) 事件发生的日期和时间；

b) 事件主体；

c) 事件客体；

d) 事件描述；

e) 事件类型；

f) 事件级别；

g) 日志数据源的 IP 地址或名称。

4.1.5 日志记录存储

4.1.5.1 安全保护

日志分析产品应采取安全机制，保护日志记录免遭未经授权的读取、删除或修改。

4.1.5.2 防止日志记录丢失

日志分析产品应提供以下措施防止日志记录丢失：

a) 日志记录应存储于掉电非易失性存储介质中；

b) 当日志记录的存储容量达到阈值时，发出报警信息；

c) 在日志记录的存储空间耗尽前，采用自动转储的方式将日志记录自动备份到其他的存储空间。

4.1.6 日志记录备份

日志分析产品应提供以下日志记录备份功能：

a) 支持可定制的自动化备份功能及策略；

b) 支持异地备份。

4.2 日志分析和处理

4.2.1 日志记录处理

4.2.1.1 数据整合

日志分析产品应能检查日志记录是否重复或无效，并进行数据的整合，即采用一定的技术手段对日志记录进行去重和有效性检查，以保证数据的有效性、一致性，以及减少冗余信息。

4.2.1.2 数据拆分

若日志记录的单一字段包含多种信息并且这多种信息间具有分隔符，日志分析产品应能将此单一字段拆分成便于分析的若干字段存储。

4.2.2 日志记录分析

4.2.2.1 事件辨别

日志分析产品应能动态地维护一个事件库，对网络中的各种事件根据一定的特征进行分类，并且应能对采集的日志数据进行分析，判断日志数据所属的事件类型。

4.2.2.2 事件定级

日志分析产品应为不同类型的事件设定其级别，以表明事件的性质或揭示此类事件的发生给信息系统所带来危险程度。

4.2.2.3 事件统计

日志分析产品应能够根据事件的以下属性进行统计：

a) 事件主体；
b) 事件客体；
c) 事件类型；
d) 事件级别；
e) 事件发生的日期和时间；
f) 日志数据源的 IP 地址或名称；
g) 事件的其他属性或属性的组合。

4.2.2.4 潜在危害分析

日志分析产品应能设定单类事件累计发生次数或发生频率的阈值，当统计分析表明此类事件超出阈值时则表明信息系统出现了潜在的危害。

4.2.2.5 异常行为分析

日志分析产品应维护一个与信息系统相关的合法用户的正常行为集合，以此区分入侵者的行为和合法用户的异常行为。

4.2.2.6 关联事件分析

日志分析产品应提供以下关联分析功能：

a) 根据事件的级别、事件的累计发生次数等指标进行综合分析，从而对信息系统或信息系统中单个资源的风险等级进行评估；
b) 通过对多个日志数据源进行关联事件分析应能分析到多步访问行为，并能根据已知的事件序列以图示方法模拟出完整的访问路径。

4.2.2.7 日志记录数据挖掘

日志分析产品应能够从大量的日志数据中提取隐含的、事先未知的、具有潜在价值的有用信息和知识，具体要求如下：

a) 提取同一类型的事件的共同性质，如事件频繁发生的时间段等；
b) 提取单个事件和其他事件之间依赖或关联的知识，如事件发生的因果关系等；
c) 提取反映同类事件共同性质的特征和不同事件之间的差异型特征，揭示隐含事件的发生；
d) 发现其他类型的知识，揭示偏离常规的异常现象；
e) 根据数据的时间序列，由历史的和当前的数据去推测未来的数据，比如分析某一目标系统的用户访问日志，从中寻找用户普遍访问的规律。

4.3 日志呈现和报警

4.3.1 日志查询

日志分析产品应能够根据事件的以下属性进行日志记录查询：

a) 事件主体；
b) 事件客体；
c) 事件类型；
d) 事件级别；
e) 事件发生的日期和时间；
f) 日志数据源的 IP 地址或名称；
g) 事件的其他属性或属性的组合。

4.3.2 统计报表

日志分析产品应能够根据事件统计结果生成统计报表，并能以通用格式输出。

4.3.3 分析报告

日志分析产品应能根据日志记录分析结果生成分析报告，并能够以通用格式输出，分析报告应包含以下内容：

a) 日志记录分析结果；
b) 对信息系统或信息系统中单个资源的风险等级提供评估结果；
c) 对日志记录分析结果提供补救建议；
d) 根据日志数据挖掘收集到的知识，提供预测性的信息。

4.3.4 报警机制

日志分析产品应能针对以下事件，进行报警：

a) 用户指定的事件，如高危险级别的事件等；
b) 潜在危害分析结果表明信息系统存在潜在危害；
c) 异常行为分析结果表明信息系统存在入侵者的行为或合法用户的异常行为；
d) 日志记录分析结果表明信息系统或信息系统中某一资源存在风险。

4.4 开发接口

日志分析产品应至少提供一个标准的、开放的接口，能按照该接口的规范为其他信息安全产品编写相应的程序模块，以便共享信息或规范化联动。

5 自身安全功能要求

5.1 组件安全

5.1.1 日志代理安全

5.1.1.1 软件代理的自保护能力

日志分析产品应对软件代理采取以下的保护措施：

a) 防止非授权用户强行终止软件代理运行；
b) 防止非授权用户强制取消软件代理在系统启动时自动加载；
c) 防止非授权用户强行卸载、删除或修改软件代理。

5.1.1.2 日志代理状态监视

日志管理中心应能监视日志代理的状态，并在审计日志中记录日志代理的状态变更。

5.1.1.3 数据传输控制

日志分析产品应确保只有授权管理员能决定数据传输的启动或终止。

5.1.1.4 数据续传

当日志代理与日志管理中心连接出现故障时，日志分析产品应有一定的措施防止日志数据丢失，确保在连接恢复正常之后日志数据能够续传到日志管理中心。

5.1.2 集中管理

日志分析产品应能够集中定制日志采集策略，并分发应用到相应的日志代理上。

5.1.3 数据传输安全

若日志分析产品组件间通过网络进行通讯，日志分析产品应对组件间相互传输的数据进行保护，保证数据在传送过程中的完整性和保密性。

5.1.4 时间同步

日志分析产品应提供时间同步功能，保证日志分析产品组件之间时间的一致性。

5.2 安全管理

5.2.1 标识和鉴别

5.2.1.1 唯一性标识

日志分析产品应为用户提供唯一标识，同时将用户的身份标识与该用户的所有可审计事件相关联。

5.2.1.2 身份鉴别

日志分析产品应在执行任何与安全功能相关的操作之前对用户进行鉴别。

5.2.1.3 鉴别数据保护

日志分析产品应保证鉴别数据不被未授权查阅或修改。

5.2.1.4 鉴别失败处理

当用户鉴别失败的次数达到设定值时，日志分析产品应按以下措施处理：

a) 终止会话；
b) 锁定用户账号或远程登录主机的地址；
c) 产生系统报警消息，通知授权管理员。

5.2.2 安全功能管理

日志分析产品应为授权管理员提供以下管理功能：

a) 查看和修改各种安全属性；
b) 定制和修改各种安全策略。

5.2.3 区分安全角色管理

日志分析产品应能通过对授权管理员给以不同的角色配置，赋予授权管理员不同的管理权限。

5.2.4 远程管理

若日志分析产品提供远程管理功能，应采取以下措施保证远程管理安全：

a) 对远程管理信息进行保密传输；

b) 对可信主机的地址进行限制。

5.3 自身审计功能

5.3.1 审计日志生成

日志分析产品应对以下事件生成审计日志：

a) 管理员的登录事件，包括成功和失败；

b) 对安全策略进行更改的操作；

c) 因鉴别尝试不成功的次数达到设定值导致的会话连接终止；

d) 对日志记录的备份和删除；

e) 日志代理状态的变更；

f) 对安全角色进行增加、删除和属性修改的操作；

g) 管理员的其他操作。

应在每一条审计日志中记录事件发生的日期、时间、用户标识、事件描述和结果。若日志分析产品提供远程管理功能，还应记录远程登录主机的地址。

5.3.2 审计日志存储

日志分析产品应将审计日志存储于掉电非易失性存储介质中。

5.3.3 审计日志管理

日志分析产品应只允许授权管理员访问审计日志，并为授权管理员提供审计日志查询、备份、删除和清空功能。

5.4 系统报警

5.4.1 报警事件类型

日志分析产品应能对以下系统事件进行报警：

a) 日志代理状态异常；

b) 日志记录的存储空间达到设定值；

c) 用户鉴别失败的次数达到设定值；

d) 授权管理员自定义的其他系统事件。

5.4.2 报警消息

日志分析产品的报警消息内容应满足以下要求：

a) 为管理员可理解；

b) 至少包括事件发生的日期、时间、事件主体和事件描述。

5.4.3 报警方式

日志分析产品的报警方式应包含以下方式中的一种或多种：

a) 弹出报警窗口；

b) 发送报警邮件；
c) 发送 Snmp trap 消息；
d) 发送声光电信号；
e) 发送 SMS 短消息。

6 安全保证要求

6.1 配置管理

6.1.1 配置管理能力

6.1.1.1 版本号

开发者应为产品的不同版本提供唯一的标识。

6.1.1.2 配置项

开发者应使用配置管理系统并提供配置管理文档。

配置管理文档应包括一个配置清单，配置清单应唯一标识组成产品的所有配置项并对配置项进行描述。

配置管理文档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。

6.1.1.3 授权控制

开发者提供的配置管理文档应包括一个配置管理计划，配置管理计划应描述如何使用配置管理系统。实施的配置管理应与配置管理计划相一致。

开发者应提供所有的配置项得到有效地维护的证据。

开发者应保证只有经过授权才能修改配置项。

6.1.2 配置管理覆盖

配置管理范围至少应包括产品交付与运行文档、开发文档、指导性文档、生命周期支持文档、测试文档、脆弱性分析文档和配置管理文档，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。

配置管理文档至少应能跟踪上述内容，并描述配置管理系统是如何跟踪这些配置项的。

6.2 交付与运行

6.2.1 交付程序

开发者应使用一定的交付程序交付产品，并将交付过程文档化。

交付文档应描述在给用户方交付产品的各版本时，为维护安全所必需的所有程序。

6.2.2 安装、生成和启动程序

开发者应提供文档说明产品的安装、生成和启动的过程。

6.3 开发

6.3.1 非形式化功能规范

开发者应提供一个功能规范，使用非形式化风格来描述产品安全功能及其外部接口。

功能规范应是内在一致的，应描述所有外部接口的用途与使用方法，适当时应提供效果、例外情况和错误消息的细节，并完备地表示产品的功能。

6.3.2 高层设计

6.3.2.1 描述性高层设计

开发者应提供产品安全功能的高层设计。

高层设计应以非形式风格表述并且是内在一致的。为说明安全功能的结构，高层设计应将安全功能分解为各个安全功能子系统进行描述。对于每一个安全功能子系统，高层设计应描述其提供的安全功能，标识其所有接口以及哪些接口是外部可见的，描述其所有接口的使用目的和方法。高层设计还应标识安全功能要求的所有基础性的硬件、固件和软件，并且支持由这些硬件、固件和软件实现的保护机制。

6.3.2.2 安全加强的高层设计

开发者应阐明如何将有助于产品安全功能的子系统和其他子系统分开，并适当提供安全功能子系统的作用、例外情况和错误消息的细节。

6.3.3 非形式化对应性证实

开发者应在产品安全功能表示的所有相邻对之间提供对应性分析。

对于产品安全功能表示的每个相邻对，分析应阐明：较为抽象的安全功能表示的所有相关安全功能，应在较具体的安全功能表示中得到正确且完备地细化。

6.4 指导性文档

6.4.1 管理员指南

开发者应提供管理员指南，管理员指南应与为评估而提供的其他所有文档保持一致。

管理员指南应说明以下内容：

a) 管理员可使用的管理功能和接口；
b) 怎样安全地管理产品；
c) 在安全处理环境中应被控制的功能和权限；
d) 所有对与产品的安全操作有关的用户行为的假设；
e) 所有受管理员控制的安全参数，如果可能，应指明安全值；
f) 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实体的安全特性进行的改变；
g) 所有与管理员有关的 IT 环境安全要求。

6.4.2 用户指南

开发者应提供用户指南，用户指南应与为评估而提供的其他所有文档保持一致。

用户指南应说明以下内容：

a) 产品的非管理员用户可使用的安全功能和接口；
b) 产品提供给用户的安全功能和接口的使用方法；
c) 用户可获取受安全处理环境所控制的所有功能和权限；
d) 产品安全操作中用户所应承担的职责；
e) 与用户有关的 IT 环境的所有安全要求。

6.5 生命周期支持

开发者应提供开发安全文档。

开发安全文档应描述在产品的开发环境中，为保护产品设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施。

开发安全文档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。

6.6 测试

6.6.1 覆盖

6.6.1.1 覆盖证据

开发者应提供测试覆盖的证据。

在测试覆盖证据中，应表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能是对应的。

6.6.1.2 覆盖分析

开发者应提供测试覆盖的分析结果。

测试覆盖的分析结果应表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能之间的对应性是完备的。

6.6.2 测试深度

开发者应提供测试深度的分析。

在深度分析中，应说明测试文档中所标识的对安全功能的测试，足以表明该安全功能和高层设计是一致的。

6.6.3 功能测试

开发者应测试安全功能，将结果文档化并提供测试文档。

测试文档应包括测试计划、测试过程、预期的测试结果和实际的测试结果。

测试计划应标识要测试的安全功能，并描述测试的目标。

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，这些概况应包括对于其他测试结果的顺序依赖性。

预期的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。

6.6.4 独立测试

6.6.4.1 一致性

开发者应提供适合测试的产品，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。

6.6.4.2 抽样

开发者应提供一组相当的资源，用于安全功能的抽样测试。

6.7 脆弱性分析保证

6.7.1 指南审查

开发者应提供指南性文档。

在指南性文档中，应确定对产品的所有可能的操作方式(包括失败或失误后的操作)、它们的后果以及对于保持安全操作的意义。

指南性文档还应列出所有目标环境的假设以及所有外部安全措施(包括外部程序的、物理的或人员的控制)要求。

指南性文档应是完备的、清晰的、一致的、合理的。

6.7.2 安全功能强度评估

开发者应对指导性文档中所标识的每个具有安全功能强度声明的安全机制进行安全功能强度分析，说明该安全机制达到或超过指导性文档中定义的最低强度级别和特定功能强度度量。

6.7.3 开发者脆弱性分析

开发者应执行脆弱性分析，并提供脆弱性分析文档。

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。

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。

7 等级划分要求

7.1 概述

依据日志分析相关产品的开发、生产现状及实际应用情况，将日志分析安全功能要求、自身安全功能要求和安全保证要求划分成三个等级。

7.2 安全功能要求等级划分

日志分析产品的安全功能要求等级划分如表1所示。

表1 日志分析产品安全功能要求等级划分

安全功能要求			第一级	第二级	第三级
日志采集和存储	日志数据源		4.1.1a)～4.1.1c)	4.1.1	4.1.1
	日志数据采集	标准协议接收	4.1.2.1	4.1.2.1	4.1.2.1
		代理方式采集	4.1.2.2	4.1.2.2	4.1.2.2
		日志文件导入	—	—	4.1.2.3
		日志采集及时性	4.1.2.4	4.1.2.4	4.1.2.4
	日志数据的预处理	数据筛选	4.1.3.1	4.1.3.1	4.1.3.1
		数据转换	4.1.3.2	4.1.3.2	4.1.3.2
	日志记录生成		4.1.4	4.1.4	4.1.4
	日志记录存储	安全保护	4.1.5.1	4.1.5.1	4.1.5.1
		防止日志记录丢失	4.1.5.2a)、4.1.5.2b)	4.1.5.2	4.1.5.2
	日志记录备份		4.1.6a)	4.1.6	4.1.6

表 1（续）

安全功能要求			第一级	第二级	第三级
日志实现和报警	日志记录处理	数据整合	—	4.2.1.1	4.2.1.1
		数据拆分	—	—	4.2.1.2
	日志记录分析	事件辨别	4.2.2.1	4.2.2.1	4.2.2.1
		事件定级	4.2.2.2	4.2.2.2	4.2.2.2
		事件统计	4.2.2.3a)～4.2.2.3f)	4.2.2.3	4.2.2.3
		潜在危害分析	4.2.2.4	4.2.2.4	4.2.2.4
		异常行为分析	—	4.2.2.5	4.2.2.5
		关联事件分析	—	4.2.2.6a)	4.2.2.6
		日志记录数据挖掘	—	4.2.2.7a)～4.2.2.7c)	4.2.2.7
	日志查询		4.3.1a)～4.3.1f)	4.3.1	4.3.1
	统计报表		4.3.2	4.3.2	4.3.2
	分析报告		—	4.3.3a)、4.3.3b)	4.3.3
	报警机制		4.3.4a)、4.3.4b)	4.3.4	4.3.4
开发接口			—	—	4.4

7.3 自身安全功能要求等级划分

日志分析产品的自身安全功能要求等级划分如表 2 所示。

表 2 日志分析产品自身安全功能要求等级划分

自身安全功能要求			第一级	第二级	第三级
组件安全	日志代理安全	软件代理的自保护能力	5.1.1.1	5.1.1.1	5.1.1.1
		日志代理状态监视	5.1.1.2	5.1.1.2	5.1.1.2
		数据传输控制	5.1.1.3	5.1.1.3	5.1.1.3
		数据续传	5.1.1.4	5.1.1.4	5.1.1.4
	集中管理		—	5.1.2	5.1.2
	数据传输安全		—	5.1.3	5.1.3
	时间同步		—	5.1.4	5.1.4
安全管理	标识和鉴别	唯一性标识	5.2.1.1	5.2.1.1	5.2.1.1
		身份鉴别	5.2.1.2	5.2.1.2	5.2.1.2
		鉴别数据保护	5.2.1.3	5.2.1.3	5.2.1.3
		鉴别失败处理	—	5.2.1.4a)、5.2.1.4b)	5.2.1.4
	安全功能管理		5.2.2	5.2.2	5.2.2
	区分安全角色管理		—	5.2.3	5.2.3
	远程管理		—	5.2.4	5.2.4

表 2（续）

自身安全功能要求		第一级	第二级	第三级
自身审计功能	审计日志生成	5.3.1a)～5.3.1e)	5.3.1a)～5.3.1f)	5.3.1
	审计日志存储	5.3.2	5.3.2	5.3.2
	审计日志管理	5.3.3	5.3.3	5.3.3
系统报警	报警事件类型	5.4.1a)、5.4.1b)	5.4.1a)、5.4.1b)	5.4.1
	报警消息	5.4.2	5.4.2	5.4.2
	报警方式	5.4.3	5.4.3	5.4.3

7.4 安全保证要求等级划分

日志分析产品的安全保证要求等级划分如表 3 所示。

表 3 日志分析产品安全保证要求等级划分

安全功能要求			第一级	第二级	第三级
配置管理	配置管理能力	版本号	6.1.1.1	6.1.1.1	6.1.1.1
		配置项	—	6.1.1.2	6.1.1.2
		授权控制	—	—	6.1.1.3
	配置管理覆盖		—	—	6.1.2
交付与运行	交付程序		—	6.2.1	6.2.1
	安装、生成和启动程序		6.2.2	6.2.2	6.2.2
开发	非形式化功能规范		6.3.1	6.3.1	6.3.1
	高层设计	描述性高层设计	—	6.3.2.1	6.3.2.1
		安全加强的高层设计	—	—	6.3.2.2
	非形式化对应性证实		6.3.3	6.3.3	6.3.3
指导性文档	管理员指南		6.4.1	6.4.1	6.4.1
	用户指南		6.4.2	6.4.2	6.4.2
生命周期支持			—	—	6.5
测试	覆盖	覆盖证据	—	6.6.1.1	6.6.1.1
		覆盖分析	—	—	6.6.1.2
	测试深度		—	—	6.6.2
	功能测试		—	6.6.3	6.6.3
	独立测试	一致性	6.6.4.1	6.6.4.1	6.6.4.1
		抽样	—	6.6.4.2	6.6.4.2
脆弱性分析保证	指南审查		—	—	6.7.1
	安全功能强度评估		—	6.7.2	6.7.2
	开发者脆弱性分析		—	6.7.3	6.7.3

中华人民共和国公共安全
行业标准
信息安全技术
日志分析产品安全技术要求
GA/T 911—2010
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1.25 字数 28 千字
2011年2月第一版 2011年2月第一次印刷
*
书号:155066·2-21420 定价 21.00元

BZ 0100648

打印日期:2013年7月30日 F055A