ICS 35.240
A.90

GA

中华人民共和国公共安全行业标准

GA/T XXXX—XXXX
代替 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 technical requirements for log analysis products

（报批稿）

XXXX－XX－XX 发布 XXXX－XX－XX 实施

中华人民共和国公安部 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　总体说明 2
4.1　安全技术要求分类 2
4.2　安全等级划分 2
5　安全功能要求 2
5.1　日志采集和存储 2
5.2　日志分析和处理 4
5.3　日志呈现和报警 5
5.4　开发接口 6
6　自身安全功能要求 6
6.1　组件安全 6
6.2　安全管理 6
6.3　自身审计功能 7
6.4　系统报警 8
7　安全保障要求 8
7.1　开发 8
7.2　指导性文档 9
7.3　生命周期支持 10
7.4　测试 11
7.5　脆弱性评定 11
8　等级划分要求 12
8.1　概述 12
8.2　安全功能要求等级划分 12
8.3　自身安全功能要求等级划分 13
8.4　安全保障要求等级划分 13

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准代替GA/T 911-2010《信息安全技术 日志分析产品安全技术要求》，与GA/T 911-2010相比主要变化如下：

——修改了“等级划分”的要求，将等级划分为基本级和增强级两级（见第8章，2010年版的7.2、7.3和7.4）；

——删除了“标准协议接收”的要求（见2010年版的4.1.2.1）；

——删除了“代理方式采集”的要求（见2010年版的4.1.2.2）；

——删除了“日志文件导入”的要求（见2010年版的4.1.2.3）；

——增加了“数据采集”的要求（见5.1.2.1）；

——修改了“审计记录备份”的要求（见5.1.6，2010年版的4.2.3）；

——删除了“软件代理的自保护能力”的要求（见2010年版的5.1.1.1）；

——删除了“数据传输控制”的要求（见2010年版的5.1.1.3）；

——删除了“数据续传”的要求（见2010年版的5.1.1.4）；

——增加了“多级部署”的要求（见6.1.1）；

——增加了“多重鉴别”的要求（见6.2.1.3）；

——增加了“超时锁定”的要求（见6.2.1.4）；

——删除了“审计记录存储”的要求（见2010年版的5.3.2）；

——删除了“审计管理”的要求（见2010年版的5.3.3）；

——增加了“数据存储安全”的要求（见6.3.3）。

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、杭州安恒信息技术有限公司、华为技术有限公司。

本标准主要起草人：陈卓、张笑笑、陆臻、唐迪、俞优、沈亮、吴其聪。

本标准的历次版本发布情况为：

——GA/T 911-2010。

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、安全保障要求及等级划分要求。

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 18336.3-2015 信息技术 安全技术 信息技术安全评估准则 第3部分：安全保障组件

GB/T 25069-2010 信息安全技术 术语

3 术语和定义

GB/T 18336.3-2015和GB/T 25069-2010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。

3.4

审计日志 audit log

日志分析产品自身审计产生的日志数据。

3.5

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。

3.6

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。

4 总体说明

4.1 安全技术要求分类

本标准将日志分析产品安全技术要求分为安全功能、自身安全功能和安全保障要求三大类。其中，安全功能要求是对日志分析产品应具备的安全功能提出具体要求，包括日志采集和存储、日志记录处理、日志呈现和报警和开发接口等；自身安全功能是对日志分析产品应具备的自身安全功能提出具体要求，包括组件安全、安全管理、自身审计功能和系统报警等；安全保障要求针对日志分析产品的生命周期过程提出具体的要求，例如开发、指导性文档、生命周期支持、测试和脆弱性评定等。

4.2 安全等级划分

日志分析产品的安全等级按照其安全功能要求、自身安全功能要求和安全保障要求的强度划分为基本级和增强级，其中安全保障要求参考了GB/T 18336.3—2015。

5 安全功能要求

5.1 日志采集和存储

5.1.1 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；
b） 操作系统；
c） 数据库系统；
d） 其他应用系统。

5.1.2 日志数据采集

5.1.2.1 数据采集

日志分析产品应能通过一定的方式采集日志数据源的日志数据，至少包括以下一种采集方式：

a） 日志代理；

b） 标准协议；

c） 文件导入；

d） 其他。

5.1.2.2 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。

5.1.3 日志数据的预处理

5.1.3.1 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。

5.1.3.2 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和损坏。

5.1.4 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、MAC 或名称。

5.1.5 日志记录存储

5.1.5.1 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。

5.1.5.2 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自动将较早日志记录转存到其他设备上。

5.1.6 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） 通过自动方式对日志记录进行转存，实现异地备份。

5.2 日志分析和处理

5.2.1 日志记录处理

5.2.1.1 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。

5.2.1.2 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。

5.2.2 日志记录分析

5.2.2.1 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。

5.2.2.2 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。

5.2.2.3 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。

5.2.2.4 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。

5.2.2.5 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。

5.2.2.6 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。

5.2.2.7 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。

5.3 日志呈现和报警

5.3.1 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。

5.3.2 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。

5.3.3 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。

5.3.4 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。

5.4 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。

6 自身安全功能要求

6.1 组件安全

6.1.1 日志代理状态监测

日志分析产品应能监测日志代理的在线状态。

6.1.2 多级部署

日志分析产品应支持分布式多级方式部署。

6.1.3 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。

6.1.4 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。

6.1.5 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。

6.2 安全管理

6.2.1 标识和鉴别

6.2.1.1 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。

6.2.1.2 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。

6.2.1.3 多重鉴别

日志分析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。

6.2.1.4 超时锁定

日志分析产品应具有登录超时锁定或注销功能。在设定的时间段内没有任何操作的情况下，终止会话，需要再次进行身份鉴别才能够重新操作。最大超时时间仅由授权管理员设定。

6.2.1.5 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。

6.2.1.6 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。

6.2.2 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。

6.2.3 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。

6.2.4 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） 对远程登录主机的地址进行限制。

6.3 自身审计功能

6.3.1 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。

6.3.2 数据存储安全

日志分析产品应防止审计数据被删除或篡改，保证存储数据的完整性。

6.4 系统报警

6.4.1 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） 日志记录的存储空间达到设定值；
b） 用户鉴别失败的次数达到设定值；
c） 授权管理员自定义的其他系统事件。

6.4.2 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。

6.4.3 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。

7 安全保障要求

7.1 开发

7.1.1 安全架构

开发者应提供产品安全功能的安全架构描述，安全架构描述应满足以下要求：

a） 与产品设计文档中对安全功能实施抽象描述的级别一致；

b） 描述与安全功能要求一致的产品安全功能的安全域；

c） 描述产品安全功能初始化过程为何是安全的；

d） 证实产品安全功能能够防止被破坏；

e） 证实产品安全功能能够防止安全特性被旁路。

7.1.2 功能规范

开发者应提供完备的功能规范说明，功能规范说明应满足以下要求：

a） 完全描述产品的安全功能；

b） 描述所有安全功能接口的目的与使用方法；

c） 标识和描述每个安全功能接口相关的所有参数；

d） 描述安全功能接口相关的安全功能实施行为；

e） 描述由安全功能实施行为处理而引起的直接错误消息；

f） 证实安全功能要求到安全功能接口的追溯；

g） 描述安全功能实施过程中，与安全功能接口相关的所有行为；

h） 描述可能由安全功能接口的调用而引起的所有直接错误消息。

7.1.3 实现表示

开发者应提供全部安全功能的实现表示，实现表示应满足以下要求：

a） 提供产品设计描述与实现表示实例之间的映射，并证明其一致性；

b） 按详细级别定义产品安全功能，详细程度达到无须进一步设计就能生成安全功能的程度；

c） 以开发人员使用的形式提供。

7.1.4 产品设计

开发者应提供产品设计文档，产品设计文档应满足以下要求：

a） 根据子系统描述产品结构；

b） 标识和描述产品安全功能的所有子系统；

c） 描述安全功能所有子系统间的相互作用；

d） 提供的映射关系能够证实设计中描述的所有行为能够映射到调用它的安全功能接口；

e） 根据模块描述安全功能；

f） 提供安全功能子系统到模块间的映射关系；

g） 描述所有安全功能实现模块，包括其目的及与其他模块间的相互作用；

h） 描述所有实现模块的安全功能要求相关接口、其他接口的返回值、与其他模块间的相互作用及调用的接口；

i） 描述所有安全功能的支撑或相关模块，包括其目的及与其他模块间的相互作用。

7.2 指导性文档

7.2.1 操作用户指南

开发者应提供明确和合理的操作用户指南，操作用户指南与为评估而提供的其他所有文档保持一致，对每一种用户角色的描述应满足以下要求：

a） 描述在安全处理环境中被控制的用户可访问的功能和特权，包含适当的警示信息；
b） 描述如何以安全的方式使用产品提供的可用接口；
c） 描述可用功能和接口，尤其是受用户控制的所有安全参数，适当时指明安全值；
d） 明确说明与需要执行的用户可访问功能有关的每一种安全相关事件，包括改变安全功能所控制实体的安全特性；
e） 标识产品运行的所有可能状态（包括操作导致的失败或者操作性错误），以及它们与维持安全运行之间的因果关系和联系；
f） 充分实现安全目的所必须执行的安全策略。

7.2.2 准备程序

开发者应提供产品及其准备程序，准备程序描述应满足以下要求：

a） 描述与开发者交付程序相一致的安全接收所交付产品必需的所有步骤；
b） 描述安全安装产品及其运行环境必需的所有步骤。

7.3 生命周期支持

7.3.1 配置管理能力

开发者的配置管理能力应满足以下要求：

a） 为产品的不同版本提供唯一的标识；
b） 使用配置管理系统对组成产品的所有配置项进行维护，并唯一标识配置项；
c） 提供配置管理文档，配置管理文档描述用于唯一标识配置项的方法；
d） 配置管理系统提供一种自动方式来支持产品的生成，通过该方式确保只能对产品的实现表示进行已授权的改变；
e） 配置管理文档包括一个配置管理计划，配置管理计划描述如何使用配置管理系统开发产品。实施的配置管理与配置管理计划相一致；
f） 配置管理计划描述用来接受修改过的或新建的作为产品组成部分的配置项的程序。

7.3.2 配置管理范围

开发者应提供产品配置项列表，并说明配置项的开发者。配置项列表应包含以下内容：

a） 产品、安全保障要求的评估证据和产品的组成部分；
b） 实现表示、安全缺陷报告及其解决状态。

7.3.3 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。在给用户方交付产品的各版本时，交付文档应描述为维护安全所必需的所有程序。

7.3.4 开发安全

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。

7.3.5 生命周期定义

开发者应建立一个生命周期模型对产品的开发和维护进行的必要控制，并提供生命周期定义文档描述用于开发和维护产品的模型。

7.3.6 工具和技术

开发者应明确定义用于开发产品的工具，并提供开发工具文档无歧义地定义实现中每个语句的含义和所有依赖于实现的选项的含义。

7.4 测试

7.4.1 测试覆盖

开发者应提供测试覆盖文档，测试覆盖描述应满足以下要求：

a） 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间的对应性；

b） 表明上述对应性是完备的，并证实功能规范中的所有安全功能接口都进行了测试。

7.4.2 测试深度

开发者应提供测试深度的分析。测试深度分析描述应满足以下要求：

a） 证实测试文档中的测试与产品设计中的安全功能子系统和实现模块之间的一致性；

b） 证实产品设计中的所有安全功能子系统、实现模块都已经进行过测试。

7.4.3 功能测试

开发者应测试产品安全功能，将结果文档化并提供测试文档。测试文档应包括以下内容：

a） 测试计划，标识要执行的测试，并描述执行每个测试的方案，这些方案包括对于其他测试结果的任何顺序依赖性；

b） 预期的测试结果，表明测试成功后的预期输出；

c） 实际测试结果和预期的一致性。

7.4.4 独立测试

开发者应提供一组与其自测安全功能时使用的同等资源，以用于安全功能的抽样测试。

7.5 脆弱性评定

基于已标识的潜在脆弱性，产品能够抵抗以下攻击行为：

a） 具有基本攻击潜力的攻击者的攻击；

b） 具有增强型基本攻击潜力的攻击者的攻击。

8 不同安全等级的要求

8.1 安全功能要求

不同安全等级的日志分析产品的安全功能要求如表1所示。

表 1 不同安全等级的日志分析产品的安全功能要求

安全功能要求			基本级	增强级
日志采集和存储	日志数据源		5.1.1 a)~c)	5.1.1
	日志数据采集	数据采集	5.1.2.1	5.1.2.1
		日志采集及时性	5.1.2.2	5.1.2.2
	日志数据的预处理	数据筛选	5.1.3.1	5.1.3.1
		数据转换	5.1.3.2	5.1.3.2
	日志记录生成		5.1.4	5.1.4
	日志记录存储	安全保护	5.1.5.1	5.1.5.1
		防止日志记录丢失	5.1.5.2 a) b)	5.1.5.2
	日志记录备份		5.1.6 a)	5.1.6
日志处理和分析	日志记录处理	数据整合	——	5.2.1.1
		数据拆分	——	5.2.1.2
	日志记录分析	事件辨别	5.2.2.1	5.2.2.1
		事件定级	5.2.2.2	5.2.2.2
		事件统计	5.2.2.3 a)~f)	5.2.2.3
		潜在危害分析	5.2.2.4	5.2.2.4
		异常行为分析	——	5.2.2.5
		关联事件分析	——	5.2.2.6
		日志记录数据挖掘	——	5.2.2.7
日志呈现和报警	日志查询		5.3.1 a)~f)	5.3.1
	统计报表		5.3.2	5.3.2
	分析报告		——	5.3.3
	报警机制		5.3.4 a) b	5.3.4
开发接口			——	5.4

8.2 自身安全功能要求

不同安全等级的日志分析产品的自身安全功能要求如表2所示。

表 2　不同安全等级的日志分析产品的自身安全功能要求

自身安全功能要求			基本级	增强级
组件安全	日志代理状态监测		6.1.1	6.1.1
	多级部署		——	6.1.2
	集中管理		——	6.1.3
	数据传输安全		——	6.1.4
	时间同步		——	6.1.5
安全管理	标识和鉴别	唯一性标识	6.2.1.1	6.2.1.1
		身份鉴别	6.2.1.2	6.2.1.2
		多重鉴别	——	6.2.1.3
		超时锁定	6.2.1.4	6.2.1.4
		鉴别数据保护	6.2.1.5	6.2.1.5
		鉴别失败处理	——	6.2.1.6
	安全功能管理		6.2.2	6.2.2
	区分安全角色管理		——	6.2.3
	远程管理		——	6.2.4
自身审计功能	审计日志生成		6.3.1 a)~e)	6.3.1
	数据存储安全		——	6.3.2
系统报警	报警事件类型		6.4.1 a) b)	6.4.1
	报警消息		6.4.2	6.4.2
	报警方式		6.4.3	6.4.3

8.3　安全保障要求

不同安全等级的日志分析产品的安全保障要求如表3所示。

表 3 不同安全等级的日志分析产品的安全保障要求

安全保障要求		基本级	增强级
开发	安全架构	7.1.1	7.1.1
	功能规范	7.1.2 a) ～f)	7.1.2
	实现表示	——	7.1.3
	产品设计	7.1.4 a) ～d)	7.1.4
指导性文档	操作用户指南	7.2.1	7.2.1
	准备程序	7.2.2	7.2.2

表 3（续）

安全保障要求		基本级	增强级
生命周期支持	配置管理能力	7.3.1 a) ～c)	7.3.1
	配置管理范围	7.3.2 a)	7.3.2
	交付程序	7.3.3	7.3.3
	开发安全	——	7.3.4
	生命周期定义	——	7.3.5
	工具和技术	——	7.3.6
测试	覆盖	7.4.1a)	7.4.1
	深度	——	7.4.2
	功能测试	7.4.3	7.4.3
	独立测试	7.4.4	7.4.4
脆弱性评定		7.5 a)	7.5 b)