ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 911—2019
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

2019-03-19 发布　　2019-03-19 实施

中华人民共和国公安部　　发布

目　　次

前言 …… Ⅲ
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 …… 3
5.3　日志呈现和报警 …… 5
5.4　开发接口 …… 5
6　自身安全功能要求 …… 5
6.1　组件安全 …… 5
6.2　安全管理 …… 6
6.3　自身审计功能 …… 7
6.4　系统报警 …… 7
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 …… 9
7.4　测试 …… 10
7.5　脆弱性评定 …… 10
8　不同安全等级的要求 …… 10
8.1　安全功能要求 …… 10
8.2　自身安全功能要求 …… 11
8.3　安全保障要求 …… 12

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。