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。