ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 913—2019
代替 GA/T 913—2010

信息安全技术　数据库安全审计产品安全技术要求

Information security technology—Security technology requirements for database security audit products

2019-01-13 发布　　2019-01-13 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的规则起草。

本标准代替GA/T 913—2010《信息安全技术　数据库安全审计产品安全技术要求》，与GA/T 913—2010相比主要技术变化如下：

——增加了“安全技术要求分类”和“安全等级划分”的内容(见4.1、4.2)；

——修改了“数据采集”“采集策略”“安全告警”的内容(见5.1.1、5.1.2、5.2.1，2010年版的4.1.1、4.1.4、4.2.1)；

——删除了“远程保密传输”“可信管理主机”的内容(见2010年版的5.2.3、5.2.4)；

——增加了“远程安全管理”的内容(见5.5.3)；

——将“安全功能要求”和“自身安全功能要求”统一合并为“安全功能要求”(见第5章，2010年版的第4章、第5章)；

——修改“安全保证要求”为“安全保障要求”，并调整相应内容(见第6章，2010年版的第6章)；

——级别统一划分为基本级和增强级(见第7章，2010年版的第7章)。

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(公安部第三研究所)、杭州安恒信息技术有限公司。

本标准主要起草人：俞优、陈玉成、沈亮、赵婷、李毅、顾健、顾玮、范渊、孙小平。

本标准历次版本发布情况：

——GA/T 913—2010。

信息安全技术　数据库安全审计产品安全技术要求

1　范围

本标准规定了数据库安全审计产品的安全功能要求、安全保障要求及等级划分要求。

本标准适用于数据库安全审计产品的设计、开发及测试。

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

数据库安全审计产品　database security audit product

对用户访问数据库的操作行为进行记录、分析并响应的产品。

3.2

审计记录　audit record

对用户访问数据库的操作行为进行审计产生的数据。

3.3

审计日志　audit log

对数据库安全审计产品自身行为进行审计产生的数据。

3.4

审计生成单元　audit producing unit

采集并生成审计记录的功能单元。

3.5

审计响应单元　audit responding unit

对指定的事件作出响应的功能单元。

3.6

审计处理单元 audit processing unit

对审计记录进行统计和管理的功能单元。

4　总体说明

4.1　安全技术要求分类

本标准将数据库安全审计产品安全技术要求分为安全功能要求和安全保障要求两大类。其中，安