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 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

（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　审计生成单元组件要求 2
5.2　审计响应单元组件要求 3
5.3　审计处理单元组件要求 3
5.4　标识与鉴别 4
5.5　安全管理 5
5.6　审计日志 5
6　安全保障要求 6
6.1　开发 6
6.2　指导性文档 7
6.3　生命周期支持 7
6.4　测试 8
6.5　脆弱性评定 8
7　等级划分要求 8
7.1　安全功能要求 9
7.2　安全保障要求 10

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的主要技术变化如下：

——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、邓琦、沈亮、赵婷、李毅、顾健、陈玉成、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，安全功能要求是对数据库安全审计产品应具备的安全功能提出具体要求；安全保障要求针对数据库安全审计产品的生命周期过程提出具体的要求，包括开发、指导性文档、生命周期支持和测试等。

4.2 安全等级划分

数据库安全审计产品的安全等级按照其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 审计生成单元组件要求

5.1.1 数据采集

产品应能从目标环境中至少采集数据库操作行为的以下信息：

a) 事件主体：源 IP 地址、源 MAC 地址、源端口和操作用户；
b) 事件客体：目的 IP 地址、目的 MAC 地址、目的端口和操作对象，操作对象包括数据库、数据表、数据表字段等；
c) 事件发生的日期和时间；
d) 事件类型：如数据操作类、结构操作类、事务操作类、用户管理类和其他辅助操作类等；
e) 事件描述：操作具体内容，如操作语句等；
f) 事件结果：成功或失败、影响行数、响应时间和返回行数等。

5.1.2 采集策略

产品应能根据以下条件组合设置采集策略：

a) 事件主体；
b) 事件客体；
c) 事件发生的日期和时间；
d) 事件类型；
e) 事件描述的关键字；
f) 事件结果。

5.1.3 审计记录生成

当审计事件发生时，产品应根据采集策略及时生成审计记录。

5.1.4 对系统的影响

数据采集方式和过程应不会对数据库的性能产生明显影响。

5.1.5 通信加密支持

用户采用产品支持的加密方式访问数据库时，产品宜具备采集5.1.1中信息的能力。

5.2 审计响应单元组件要求

5.2.1 安全告警

产品应能对以下异常事件进行告警：

a） 自定义违规事件，如删除重要数据、影响行和返回行超过阈值；
b） 注入攻击；
c） 数据库漏洞攻击。

5.2.2 告警内容

告警信息应至少包括以下内容：

a) 告警事件主体；
b) 告警事件客体；
c) 告警事件描述；
d) 告警事件发生的日期和时间；
e) 告警事件危险级别。

5.2.3 告警方式

产品应采用屏幕实时提示、邮件告警和短信告警等一种或多种方式进行告警。

5.2.4 响应措施

产品应采用直接阻断或联动其他网络安全产品等方式，对异常事件进行处理并记录。

5.3 审计处理单元组件要求

5.3.1 审计记录查询

5.3.1.1 有限审计查阅

产品应仅允许授权管理员访问审计记录。

5.3.1.2 可选择查询

授权管理员应能根据以下条件进行组合查询和排序：

a） 事件主体；
b） 事件客体；
c） 事件类型；
d） 事件发生的日期和时间。

5.3.2 审计记录统计

5.3.2.1 报表生成

产品应能根据以下要求生成报表：

a） 具备缺省报表模版，对审计记录、异常事件等进行统计和分析；

b） 按照事件主体、事件客体和事件类型等条件自定义报表。

5.3.2.2 报表导出

统计报表应支持常用文档格式的导出。

5.3.3 审计记录存储

5.3.3.1 审计记录保护

产品应具备安全措施防止审计记录被未授权删除、泄露和篡改。

5.3.3.2 审计记录丢失防范

产品应提供以下措施防止审计记录丢失：

a） 审计记录应存储于掉电非易失性存储介质中，默认保存时限应超过6个月；

b） 当审计记录的存储容量达到阈值时，能够通知授权管理员；

c） 在审计记录的存储空间耗尽前，采用自动转储等方式将审计记录备份到其他的存储空间。

5.3.3.3 审计记录备份

产品应提供以下审计记录备份措施：

a) 可定制的自动化备份策略；

b) 支持备份至其他存储设备。

5.3.4 会话分析

产品应能根据单条审计记录关联分析出同一会话的所有操作信息。

5.4 标识与鉴别

5.4.1 用户标识

5.4.1.1 属性定义

产品应为每个用户规定与之相关的安全属性，如标识、鉴别信息和权限等。

5.4.1.2 属性初始化

产品应提供使用默认值对创建的每个用户的属性进行初始化的能力。

5.4.1.3 唯一性标识

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。

5.4.2 身份鉴别

5.4.2.1 基本鉴别

产品应在执行任何与安全功能相关的操作之前鉴别用户的身份。

5.4.2.2 鉴别数据保护

产品应保证鉴别数据不被未授权查阅、修改。

5.4.2.3 鉴别失败处理

当对用户鉴别失败的次数达到指定次数后，产品应能终止用户的访问。

5.4.2.4 超时锁定或注销

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。

5.5 安全管理

5.5.1 安全功能管理

授权管理员应能对产品进行以下管理：

a) 查看、修改相关安全属性；
b) 启动、关闭全部或部分审计功能；
c) 制定、修改各种安全策略。

5.5.2 安全角色管理

产品应能对管理员角色进行区分：

a) 具有不同权限的管理员角色；
b) 根据不同的功能模块定义各种不同权限角色。

5.5.3 远程安全管理

若产品支持通过网络进行通信，应满足以下技术要求：

a) 防止远程会话信息被泄露和篡改；
b) 对远程管理主机的地址进行限制。

5.6 审计日志

5.6.1 审计日志生成

产品应对以下事件生成审计日志：

a) 管理员登录成功、失败；
b) 对安全策略进行更改；
c) 对管理员进行增加、删除和属性修改；
d) 对审计记录进行备份。

每一条审计日志至少应包括事件发生的日期、时间、用户标识、事件描述和结果。若采用远程登录方式对产品进行管理还应记录管理主机的地址。

5.6.2 审计日志存储

审计日志应能存储于掉电非易失性存储介质中。

5.6.3 审计日志管理

产品应提供以下审计日志管理功能：

a) 只允许授权管理员访问审计日志；
b) 对审计日志的查询功能；

c) 保存及导出审计日志。

6 安全保障要求

6.1 开发

6.1.1 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。

6.1.2 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。

6.1.3 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。

6.1.4 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。

6.2 指导性文档

6.2.1 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执行的安全策略。

6.2.2 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。

6.3 生命周期支持

6.3.1 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。

6.3.2 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。

6.3.3 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。

6.3.4 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。

6.3.5 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。

6.3.6 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。

6.4 测试

6.4.1 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。

6.4.2 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。

6.4.3 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测试结果的一致性。

6.4.4 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。

6.5 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。

7 不同安全等级的要求

7.1 安全功能要求

不同安全等级的数据库安全审计产品的安全功能要求如表 1 所示。

表1　不同安全等级的数据库安全审计产品的安全功能要求

安全功能要求			基本级	增强级
审计生成单元组件要求	数据采集		5.1.1	5.1.1
	采集策略		5.1.2 a) ～c)	5.1.2
	审计记录生成		5.1.3	5.1.3
	对系统的影响		5.1.4	5.1.4
	通信加密支持		——	5.1.5
审计响应单元组件要求	安全告警		5.2.1 a)	5.2.1
	告警内容		5.2.2	5.2.2
	告警方式		5.2.3	5.2.3
	响应措施		——	5.2.4
审计处理单元组件要求	审计记录查询	有限审计查阅	5.3.1.1	5.3.1.1
		可选择查询	5.3.1.2	5.3.1.2
	审计记录统计	报表生成	5.3.2.1 a)	5.3.2.1
		报表导出	5.3.2.2	5.3.2.2
	审计记录存储	审计记录保护	5.3.3.1	5.3.3.1
		审计记录丢失防范	5.3.3.2 a)、b)	5.3.3.2
		审计记录备份	——	5.3.3.3
	会话分析		——	5.3.4
标识与鉴别	用户标识	属性定义	5.4.1.1	5.4.1.1
		属性初始化	5.4.1.2	5.4.1.2
		唯一性标识	5.4.1.3	5.4.1.3
	身份鉴别	基本鉴别	5.4.2.1	5.4.2.1
		鉴别数据保护	5.4.2.2	5.4.2.2
		鉴别失败处理	——	5.4.2.3
		超时锁定或注销	——	5.4.2.4
安全管理	安全功能管理		5.5.1	5.5.1
	安全角色管理		5.5.2 a)	5.5.2
	远程安全传输		5.5.3 a)	5.5.3

表1 （续）

安全功能要求		基本级	增强级
审计日志	审计日志生成	5.6.1 a) ～c)	5.6.1
	审计日志存储	5.6.2	5.6.2
	审计日志管理	5.6.3	5.6.3

7.2 安全保障要求

不同安全等级的数据库安全审计产品的安全保障要求如表 2 所示。

表2 不同安全等级的数据库安全审计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	6.1.1	6.1.1
	功能规范	6.1.2 a) ～f)	6.1.2
	实现表示	——	6.1.3
	产品设计	6.1.4 a) ～d)	6.1.4
指导性文档	操作用户指南	6.2.1	6.2.1
	准备程序	6.2.2	6.2.2
生命周期支持	配置管理能力	6.3.1 a) ～c)	6.3.1
	配置管理范围	6.3.2 a)	6.3.2
	交付程序	6.3.3	6.3.3
	开发安全	——	6.3.4
	生命周期定义	——	6.3.5
	工具和技术	——	6.3.6
测试	测试覆盖	6.4.1 a)	6.4.1
	测试深度	——	6.4.2
	功能测试	6.4.3	6.4.3
	独立测试	6.4.4	6.4.4
脆弱性评定		6.5 a)	6.5 b)