ICS 35.240
A. 90

GA

中华人民共和国公共安全行业标准

GA/T 1718—2020

信息安全技术　大数据平台安全管理产品安全技术要求

Information security technology—Security technology requirements for security management products of big data platform

2020-04-02 发布　　2020-06-01 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、公安部网络安全保卫局、公安部第三研究所。

本标准主要起草人：吴其聪、张笑笑、宋好好、陆臻、俞优、沈亮。

信息安全技术　大数据平台安全管理
产品安全技术要求

1　范围

本标准规定了大数据平台安全管理产品的安全功能要求、安全保障要求和等级划分要求。

本标准适用于大数据平台安全管理产品的设计、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　信息技术安全性评估准则　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

大数据　big data

大规模的数据集，具有大量、多样、快速和/或易变的特征，需要可扩展的架构来进行有效地存储、计算和分析。

3.2

大数据平台　big data platform

对大数据进行存储和处理的软硬件系统。

3.3

审计日志　audit log

大数据平台安全管理产品自身审计产生的日志数据。

3.4

事件记录　event log

大数据平台产生的针对大数据进行访问、处理、分析等操作，并由大数据平台安全管理产品统一收集并集中存储的日志数据。

4　大数据平台安全管理产品描述

大数据平台安全管理产品(以下简称“产品”)是一个对组成大数据平台的各类软硬件系统进行集中安全管理的产品，其主要功能包括状态监测、配置管理、策略管理、数据安全访问和安全审计等，并能够通过访问控制等技术保证数据安全访问。

5 总体说明

5.1 安全技术要求分类

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，安全功能要求是对产品应具备的安全功能提出具体要求，包括安全运维、数据安全访问、安全事件响应、标识与鉴别、安全管理和安全审计等；安全保障要求针对产品的生命周期过程提出具体的要求，例如开发、指导性稳定、生命周期支持和测试等。

5.2 安全等级划分

基于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，安全保障要求级别划分应符合 GB/T 18336.3—2015 的要求。

6 安全功能要求

6.1 安全运维

6.1.1 集中部署

产品应提供集中部署功能，能够对大数据平台相关安全管理的组件进行集中安装和卸载。

6.1.2 版本检测

产品应能够获取大数据平台的软件相关版本信息。

6.1.3 补丁管理

产品应能够对大数据平台操作系统提供补丁分发功能。

6.1.4 状态监测

产品应能够实时监测各受控大数据平台的相关状态，具体包括：

a) 大数据平台各组件在线状态；
b) 硬件设备的 CPU 使用率、内存占用率、存储介质使用率、网络流量的使用情况等；
c) 业务应用的运行状态；
d) 硬件故障。

6.1.5 配置安全

产品应能够对大数据平台的配置提供以下功能：

a) 收集配置信息；
b) 提供配置备份和恢复功能；
c) 生成配置基线，并进行基线检查。

6.1.6 策略管理

产品应能够对大数据平台的安全策略进行集中管理，至少包括以下内容：

a) 数据采集策略；
b) 数据存储策略；

c） 数据备份策略；
d） 数据脱敏策略；
e） 数据访问策略。

6.2 数据安全访问

6.2.1 数据访问权限控制

产品应能够对用户访问数据的权限进行控制。若支持结构化数据，应能够按表/列控制访问权限。

6.2.2 数据脱敏

产品应能够根据预定义的策略对敏感数据进行自动扫描和检测，并根据策略进行脱敏，且满足以下要求：

a） 支持敏感数据定义；
b） 支持数据脱敏任务的制定；
c） 能够创建子集抽取规则，根据用户的要求创建比原始数据小的子集；
d） 具有抽取多表间关联子集的功能，在数据脱敏后，保持数据表之间的关联关系。

6.2.3 数据抽取和集成

产品应能够按照一定的策略进行数据抽取，并将数据抽取结果入库，控制数据的使用范围。

6.2.4 数据访问跟踪

产品应能对用户访问数据的行为进行如下跟踪：

a） 生成审计记录；
b） 对访问敏感信息的行为进行报警及阻断。

6.3 安全事件管理

6.3.1 事件记录生成

产品应能够收集各受控大数据平台所产生的日志信息，对所收集的信息统一格式，形成事件记录，并存储于掉电非易失性介质内。

6.3.2 事件记录查询

应能够对事件记录进行多条件查询，至少能按事件发生的日期和时间、事件主体、事件类型等条件进行组合。

6.3.3 统计报表

产品应能够对事件记录进行统计，按照指定条件生成汇总报表。

6.3.4 响应机制

产品应能够对日志或报警信息提供一定的响应机制，如采用 E-mail、短信或信息通知等形式通知授权管理员。

6.3.5 响应跟踪

产品能够对安全事件所处阶段进行跟踪，如告警、处理中、已处理、挂起，并满足以下要求：

a） 具备统计功能，如“已处理”安全事件数量汇总统计等；
b） 具备检测功能，告警后在指定时间范围内需要进行状态变更，对于无法进行状态变更的告知管理员或指定用户。

6.4 标识与鉴别

6.4.1 唯一性标识

产品应为用户提供唯一标识，并能将标识与其所有可审计事件相关联。

6.4.2 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。

6.4.3 多重鉴别

产品应为用户提供两种或两种以上的组合鉴别机制。

6.4.4 超时机制

产品应提供超时重新鉴别机制，如果用户停止操作的时间超过一定时限，应对用户身份重新进行鉴别。

6.4.5 口令复杂度

若产品支持口令方式进行鉴别，应能设置口令策略，对口令的长度、复杂度和有效期进行限制。

6.4.6 鉴别数据保护

产品应保证鉴别数据不被未授权查阅或修改。

6.4.7 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。

6.5 安全管理

6.5.1 安全功能管理

授权管理员应能对产品进行以下管理操作：
a） 查看、修改相关安全属性；
b） 制定和修改各种安全策略。

6.5.2 安全角色管理

产品应能对用户角色进行区分，能够根据不同的功能模块定义各种不同权限角色。

6.5.3 数据传输安全

若产品组件间通过网络进行通讯，应采取非明文传输等措施保障组件间数据传输的安全。

6.5.4 数据完整性

产品应能采取一定技术措施，保护配置信息、策略信息、监测信息的完整性。

6.5.5 可信管理主机

若控制台提供远程管理功能，应能对可远程管理的主机 IP 地址进行限制。

6.5.6 数据访问限制

产品管理员应不能通过产品访问大数据平台中的数据，所有的数据操作由后台执行。

6.5.7 数据备份

产品应能够对配置信息、审计日志进行备份和恢复。

6.6 安全审计

6.6.1 审计日志生成

产品应对与自身安全相关的事件生成审计日志：

a) 用户身份鉴别(包括成功和失败)；
b) 对用户进行增加、删除和修改属性；
c) 对安全策略、配置信息进行更改；
d) 对大数据平台数据的增加、删除和修改；
e) 对事件记录、审计日志的管理操作。

6.6.2 审计日志内容

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。

6.6.3 审计日志查阅

产品应提供审计日志查阅工具。

6.6.4 审计日志存储

审计日志存储于掉电非易失性存储介质中，并满足以下要求：

a) 能够检测或防止非授权用户对审计记录的访问；
b) 当审计日志存储空间超过阈值时，应能通知指定用户；
c) 当审计日志存储空间将要耗尽时，应采取相应的防止审计数据丢失的技术措施。

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是安全的；

d) 描述产品安全功能能够防止被破坏；

e) 描述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) 描述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用户操作指南，用户操作指南与为评估而提供的其他所有文档应保持一致，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应执行的安全策略。

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。

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） 具有增强型攻击潜力的攻击者的攻击。

8 等级划分要求

8.1 安全功能要求等级划分

产品安全功能要求等级划分如表1所示。

表1 产品安全功能要求等级划分表

安全功能要求		基本级	增强级
安全运维	集中部署	6.1.1	6.1.1
	版本检测	6.1.2	6.1.2
	补丁管理	6.1.3	6.1.3
	状态监测	6.1.4	6.1.4
	配置安全	6.1.5 a)、6.1.5 b)	6.1.5
	策略管理	6.1.6 a)～6.1.6 c)	6.1.6

表 1（续）

安全功能要求		基本级	增强级
数据安全访问	数据访问权限控制	6.2.1	6.2.1
	数据脱敏	—	6.2.2
	数据抽取和集成	—	6.2.3
	数据访问跟踪	6.2.4 a)	6.2.4
安全事件管理	事件记录生成	6.3.1	6.3.1
	事件记录查询	6.3.2	6.3.2
	统计报表	—	6.3.3
	响应机制	—	6.3.4
	响应跟踪	—	6.3.5
标识与鉴别	唯一性标识	6.4.1	6.4.1
	基本鉴别	6.4.2	6.4.2
	多重鉴别	—	6.4.3
	超时机制	—	6.4.4
	口令复杂度	—	6.4.5
	鉴别数据保护	6.4.6	6.4.6
	鉴别失败处理	6.4.7	6.4.7
安全管理	安全功能管理	6.5.1	6.5.1
	安全角色管理	—	6.5.2
	数据传输安全	6.5.3	6.5.3
	数据完整性	—	6.5.4
	可信管理主机	—	6.5.5
	数据访问限制	—	6.5.6
	数据备份	—	6.5.7
安全审计	审计日志生成	6.6.1 a)、6.6.1 b)	6.6.1
	审计日志内容	6.6.2	6.6.2
	审计日志查询	6.6.3	6.6.3
	审计日志存储	6.6.4 a)	6.6.4

8.2 安全保障要求等级划分

产品的安全保障要求等级划分如表 2 所示。

表 2　产品安全保障要求等级划分表

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)～7.1.2 f)	7.1.2
	实现表示	—	7.1.3
	产品设计	7.1.4 a)～7.1.4 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
生命周期支持	配置管理能力	7.3.1 a)～7.3.1 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	测试覆盖	7.4.1 a)	7.4.1
	测试深度	—	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

中华人民共和国公共安全
行业标准
**信息安全技术　大数据平台安全管理
产品安全技术要求**
GA/T 1718—2020
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2020年10月第一版
*
书号:155066·2-35607

GA/T 1718-2020