ICS 35.020
CCS L 80

团 体 标 准

T/CIIA 030—2022

微生物数据库安全体系设计要求

Design requirements for database security system in the field of microbiology

2022－10－20 发布　　2022－10－20 实施

中国信息协会　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国信息协会提出并归口。

本文件起草单位：中国科学院微生物研究所、中国科学院成都文献情报中心、中国科学院武汉病毒研究所、中国科学院计算机网络信息中心、广州物联网研究院、深圳华大生命科学研究院、北京携云启源科技有限公司、杭州迪安生物技术有限公司、北京微未来科技有限公司、广东美格基因科技有限公司、北京声智科技有限公司、北京神州绿盟科技有限公司、北京擎科生物科技有限公司、中国科学院东北地理与农业生态研究所农业技术中心、山东新创生物科技有限公司、中国国信信息总公司、北京蓝象标准咨询服务有限公司。

本文件主要起草人：左丽媛、孙定中、邓菲、王芳、陈方、廖方宇、胡良霖、井晓欢、张鑫磊、任绪义、王小敏、邱凯、陈孝良、陈安君、杜军、刘俊杰、于镇华、王勇、王进京、乔华阳、马建红、张德保、段小莉。

本文件为首次发布。

引　言

科学数据是国家科技创新发展和经济社会发展的重要基础性战略资源，是信息时代传播速度最快、影响面最宽、开发利用潜力最大的科技资源。科学数据信息化离不开数据库的建设，因此必须要保证数据库安全以防止数据被非法使用而造成数据的泄露、破坏和更改。微生物数据库安全体系是微生物生物安防系统的一部分，也是数据库信息安全管理系统在微生物学上的应用实例。目前，微生物数据库的安全性良莠不齐，同时从业人员也缺乏衡量这一特殊系统安全性的参考指标。

为了协助相关从业人员建立及评价微生物数据库的安全体系、保护微生物数据的信息安全，本文件从信息科学的角度明确了生物安防中关于数据的安全要求，为微生物数据库安全管理及国家科学数据安全体系建设提供支撑。微生物数据库在建立时应先进行安全风险评估，根据评估结果选择合适的安全策略，并在此基础上形成更具体的设计要求，满足不同类型、不同级别的数据库的安全要求。

微生物数据库安全体系设计要求

1 范围

本文件规定了微生物数据库安全体系设计总体要求、安全风险评估、安全策略和设计要求。

本文件适用于微生物数据库的日常维护及安全管理。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 20009—2019 信息安全技术 数据库管理系统安全评估准则

GB/T 20273—2019 信息安全技术 数据库管理系统安全技术要求

GB/T 25069—2022 信息安全技术 术语

DB33/T 2351—2021 数字化改革 公共数据分类分级指南

3 术语和定义

GB/T 20009—2019、GB/T 20273—2019、GB/T 25069—2022和DB33/T 2351—2021界定的以及下列术语和定义适用于本文件。

3.1

科学数据 scientific data

人类社会科技活动积累的或通过其他方式获取的反映客观世界的本质、特征、变化规律等原始性、基础性数据，以及根据不同科技活动需要进行系统加工整理的各类数据的集合。

[来源：GB/T 31075—2014，2.2.7]

3.2

微生物数据 microbiological data

与微生物有关的文字、数字、图形或其他形式的原始数据或产品。

3.3

微生物数据库 microbiological database

以储存微生物数据及其元数据为主的数据库及其数据库管理系统。

3.4

生物安防 biosecurity

防止生物因子及其相关处理设备、技术、数据在所有方不知情的情况下被接触或传播的措施。

3.5

生物安防风险评估 biosecurity risk assessment

对某一组织所持有的生物因子被不正当使用的风险及其后果进行评估，并制定相应的防范措施的过程。

3.6

数据安全 data security

通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

3.7

信息控制 information control

对敏感信息进行分级并按照级别确保信息的保密性和完整性的限制性措施。

4 总体要求

微生物数据库的安全需求取决于其存储的科学数据的敏感性，设计微生物数据库安全体系时应遵循以下要求：

a） 应对数据库的软硬件及科学数据本身进行安全风险评估，相关要求见第 5 章；

b） 根据评估结果选择或制定安全策略，相关要求见第 6 章；

c） 根据安全策略确定或修改数据库结构并建立一整套适用的安全体系，相关要求见第 7 章。

数据库不应存储高于其安全等级的科学数据。如果确有需要，应先对数据库进行升级以达到相应的安全要求后，再录入数据。

5 安全风险评估

5.1 数据库风险评估

数据库软硬件风险评估应遵循GB/T 20009、GB/T 20273的相关规定。

5.2 微生物数据风险评估

5.2.1 概述

微生物相关数据（例如微生物的培养环境、操作方法、来源、致病性等）可能存在潜在风险，应对其进行风险评估。根据生物安防风险评估结果，选择或制定安全策略，确定数据库结构。

5.2.2 微生物数据安全分级

5.2.2.1 分级依据

微生物数据安全分级按照生物安防风险评估结果进行划分。不同安全等级的数据形成一个偏序格。同级数据的安全等级在本体系下不能相互比较，若需要比较则应进一步细分。微生物数据安全等级可根据数据的后续处理方式进行调整。

5.2.2.2 核心数据

关系国家安全、国民经济命脉、重要民生和重大公共利益等的数据。

5.2.2.3 重要数据

一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益的数据。重要数据不包含国家秘密和未达到一定数量规模的个人信息。

5.2.2.4 一般数据

不会对国家安全、公共安全形成重要的潜在影响的数据。

6 安全策略

6.1 概述

微生物数据安全体系各部分之间的实体关系应符合图1的要求。

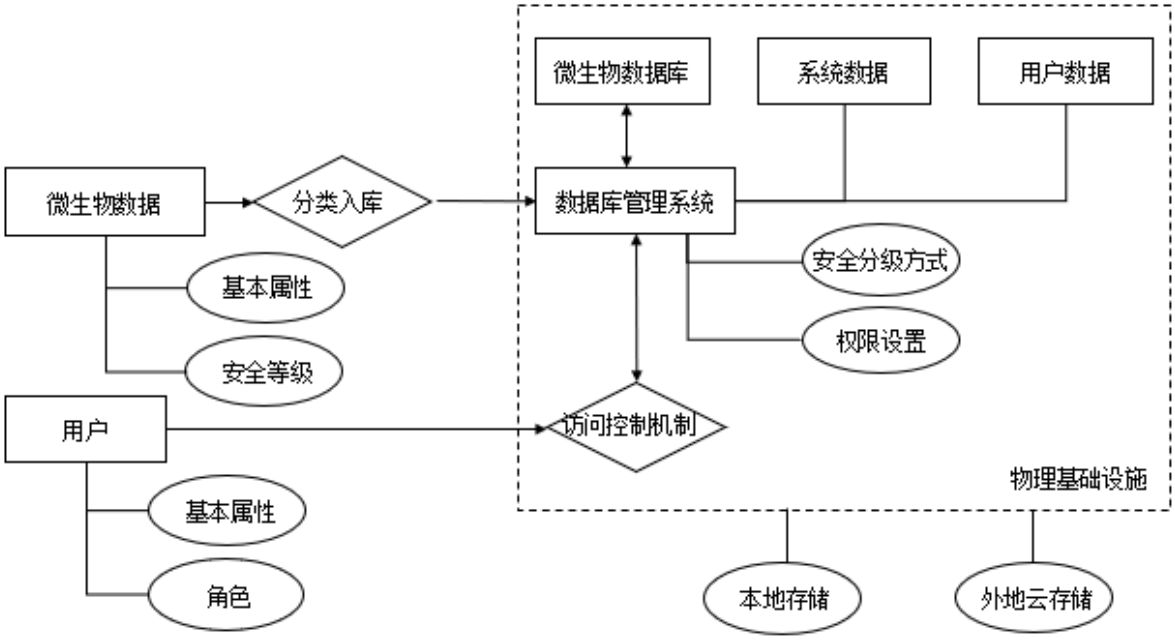

图1　微生物数据库安全体系各部分之间的实体关系图

6.2　数据分级管理

6.2.1　数据库物理基础设施

根据数据库持有数据的安全等级不同，应选择适用的数据部署方式，可供选择的数据部署方式如下：

d)　本地部署：如果数据库持有的数据以核心数据或未经脱敏的重要数据为主，应把数据集中存储在本地服务器上，严格控制数据访问。服务器所处环境应能够防止一般性的人为入侵或自然因素破坏；

e)　云部署：如果数据库所持有的数据以一般数据和公开数据为主，可选用商用云存储等分布式服务器；

f)　混合式部署：如果数据库中的数据量过于庞大，无法全部部署在本地，且又包含敏感数据，可将安全等级较高的数据存储在本地服务器上，安全等级较低的数据存放在外部的云存储上。

6.2.2　数据库管理系统

微生物数据库管理系统应对不同级别的数据实施不同的管理措施，即多级安全数据库管理系统（MLS/DBMS）。数据库应按照所辖数据的最高安全级别确立DBMS的评估保障等级（EAL）。基于GB/T 20273的相关规定，微生物数据库DBMS与其规定的EAL的对应关系如下：

a)　持有最高安全等级为核心数据的数据库，DBMS 应达到 EAL4 级；

b)　持有最高安全等级为重要数据的数据库，DBMS 应达到 EAL3 级；

c)　持有最高安全等级为一般数据的数据库，DBMS 应达到 EAL2 级；

d)　如果使用混合式数据库或云存储数据，应同时确保所采用的外部服务器的 DBMS 达到相应的 EAL。

6.3　数据分类管理

数据在进入数据库时应予以分类，并按照数据库的目的进行重新编排，以方便检索和展示。数据库提供给用户的内容应与数据库的设计初衷相适宜，不展示多余的数据。除非数据库的目的为原始数据的展示，否则未经分类的数据不应予以展示。分类示例如表1。

表1　微生物数据库数据按类划分示例

数据名称	数据类别		
	一级子类	二级子类	三级子类
微生物数据	生物学信息	生物体	分类学数据
			形态学数据
			保藏信息
			培养方法
			鉴定方法
			致病性
			用途
		生物分子	序列
			结构
			功能
	来源信息	来源环境	采集地点
			生境
		采集人/机构	——
管理系统数据	用户数据	登录信息	用户名
			密码
		权限	——
		用户个人信息	——
	系统运行数据	——	——

6.4　访问分类分级管理

6.4.1　权限

对于不同安全等级的数据，数据库应设置不同的权限要求。访问安全等级越高的数据，其所需权限也越高；同级别数据的增删改权限要求应高于查看权限要求。

根据微生物数据和元数据所属类别，可以差异化进行公开。除了根据科学研究领域以外，还可以根据其它方式（如知识产权）按照对数据库的授权情况另行聚类，在相应的安全等级下设置其他访问权限要求。

6.4.2　角色

根据微生物数据库所辖数据的敏感度和访问形式的不同，数据库应自行决定其角色设置，确保不同的角色权限有明确区分，且角色的细分程度应满足该数据库的用户需求。具体的角色设置应由微生物数据库的安全管理员根据数据库安全策略确定。

6.4.3　访问控制机制（访问监控器）

访问控制器应支持自动根据目标安全等级、用户角色以及数据库安全策略对访问请求进行分类的功能。DBMS应确保访问控制机制符合数据库的数据管理机制且无法被规避。

6.5　数据更新管理

数据更新管理应符合以下要求。

a)　数据在更新时应有可靠的校验机制，防止因多人对同一条数据重复更新而导致的数据不一致、冗余或其它错误。

b） 数据更新记录：
1） 使用专用文件或数据库，自动记录用户对数据库的所有操作；
2） 新增数据按照不同的数据分级和访问权限设定编辑权限；
3） 针对数据库结构、数据库表或字段修改，应先进行数据库备份，更新后应记录修改版本和日志。
c） 数据审核记录：
1） 针对数据条目的新增和内容的更新应配置数据审核流程；
2） 数据审核主要从完整性和准确性两个方面进行，以保障数据库高质量更新。
d） 更新和审核统计。

7 安全体系设计要求

7.1 用户身份鉴别

7.1.1 用户类型

用户类型应符合以下要求：
a） 系统管理员：能够管理数据库系统中的所有组件及数据库用户权限；
b） 数据库管理员：能够管理相关数据库中的账户、对象及数据；
c） 数据库用户：只能以特定的权限访问特定的数据库对象，不具有数据库管理权限。

7.1.2 账号设置

账号设置应符合以下要求：
a） 在系统正式使用前，数据库管理员应修改系统默认密码，并删除或锁定不需要的账号；
b） 数据库管理员具有最高数据库管理权限，其他人员应申请直接访问数据库或具有一定数据库操作权限，审批通过后，由数据库管理员告知用户权限等信息；
c） 数据库管理员为每个数据库用户建立其专门账号，以区分责任，提高系统的安全性，用户必须使用自己的账号登录数据库；
d） 对账号权限的设置应遵从最小化原则；
e） 普通数据库用户账号与数据库管理员账号分离。

7.1.3 口令策略

口令策略应符合以下要求：
a） 数据库账户口令应为无意义的字符组，长度至少 12 位，最多 32 位，并且包括数字、英文字母以及特殊字符；
b） 应根据安全要求对数据库系统的密码策略进行设置和调整，以确保口令符合要求；
c） 定期或不定期修改数据库管理口令，出现以下情况之一时，应修改数据库管理员口令：
1） 数据库正式使用前；
2） 数据库系统或相关的应用系统遭到入侵；
3） 数据库管理员轮换；
4） 数据库管理员口令泄露；
5） 其他修改口令的要求。

7.2 用户权限控制

针对每个数据库账号，按最小权限原则设置其在相应数据库中的权限。用户权限包括但不限于：
a） 系统管理权限：账户管理、服务管理、数据库管理等；
b） 数据库管理权限：创建、删除、修改数据库等；
c） 数据库访问权限：查看、检索数据库特定表记录等。

7.3 数据库对象安全

数据文件安全通过对数据文件访问权限进行控制。数据对象安全应符合以下要求：

a) 删除不需要的示例数据库，在允许存在的示例数据库中严格控制数据库账号的权限，必须存在示例数据库的情况下，尽可能使用随机模拟构建示例数据库替代；
b) 存储过程应注意删除或禁用不需要的数据存储过程；
c) 对于数据库中的敏感字段，如口令等要加密保存。

7.4 访问控制

访问控制应符合以下要求：

a) 服务及端口限制，不允许从互联网直接访问到数据库系统服务器；
b) 修改数据库系统默认监控端口；
c) 数据库连接，应用程序的数据库连接字符串中不能出现数据库账户口令明文；
d) 禁止未授权的数据库系统远程管理访问，对于已经批准的远程管理访问，应采取安全措施增强远程管理访问安全。

7.5 数据库加密

7.5.1 数据库加密

数据库加密应符合以下要求：

a) 设置加密强度，密钥应按照复杂的随机规则生成且定期更换，保证长时间且大量数据不被破译；
b) 加密后的数据库存储量没有明显的增加；
c) 加解密速度影响数据操作响应时间应尽量短；
d) 加解密对数据库的合法用户操作（如数据的增、删、改等）是透明的；
e) 建立灵活的密钥管理机制，加解密密钥存储安全，使用方便可靠。

7.5.2 加密粒度

7.5.2.1 属性加密

属性加密又称为域加密或字段加密，即以表中的列为单位进行加密。若属性的个数少于记录的条数，则需要的密钥数相对较少。若只有少数属性需要加密，则属性加密是可选的方法。

7.5.2.2 记录加密

记录加密是把表中的一条记录作为加密的单位，当数据库中需要加密的记录数较少时，可采用此方法。

7.5.2.3 数据元素加密

数据元素加密是以记录中每个字段的值为单位进行加密，数据元素是数据库中最小的加密粒度。此种加密粒度可最大限度确保系统的安全性与灵活性。

7.5.3 数据库数据加密方案

7.5.3.1 身份验证器

加密表中的数据时，加密算法将使数据变得无法阅读。此类加密的数据是无法阅读的，但可以被具有该表数据修改权限的用户操作。身份验证器是加密数据与特定数据的结合，用于确保不会发生数据行的非法移动。

7.5.3.2 对称密钥加密

解密密钥和加密密钥相同，或解密密钥由加密密钥推出。这种算法一般可分为两类，即序列算法和分组算法。序列算法一次只对明文中的单个位或字节运算；分组算法是对明文分组后以组为单位进行运算，常用有DES、SM4等。

7.5.3.3 非对称密钥加密

解密密钥不同于加密密钥，并且从解密密钥推出加密密钥在计算上是不可行的。其中加密密钥公开，解密密钥则是由用户秘密保管的私有密钥。常用的公开密钥算法有RSA、SM2等。

7.5.3.4 证书加密

证书中保存了大量的信息，包括拥有者，发布者以及有效期限。证书可以单独备份，也可以使用证书直接对数据进行加解密操作。

7.5.4 密钥安全管理

密钥安全管理机制应建立多级密钥管理体制，整个系统的密钥主要由一个主密钥、每个表上的表密钥，以及各个数据元素密钥组成。

表密钥被主密钥加密后以密文形式保存在数据字典中，数据元素密钥由主密钥及数据元素所在行、列通过某种函数自动生成，不必保存。

在多级密钥体制中，主密钥是加密子系统的关键，系统的安全性在很大程度上依赖于主密钥的安全性。

7.6 日志及监控审计

7.6.1 通用要求

日志及监控审计应符合以下通用要求：

a) 事务日志是数据库中已发生的所有修改和执行每次修改的事务的一连串记录；
b) 事务日志记录每个事务的开始，所有针对数据库的访问均有记录，通过激活实例属性，打开“安全性”选项，设定“审核级别”为全部，则登录数据库的所有账号就被详细记录在数据库日志里；
c) 通过定期查看数据库日志记录，进而检测是否存在可疑或非法的登录事件，保护数据库的安全。

7.6.2 审计范围

若数据库系统提供数据库系统管理、数据库系统账号管理及数据库管理功能，应通过配置数据库系统，将下列事件记录在日志中；若数据库系统不提供上述功能，应由数据库管理员将下列事件手工记录在日志中并存档。具体内容如下：

a) 数据库系统管理，包括但不限于系统安装、升级以及一些重要配置变更；
b) 数据库系统账户管理，包括但不限于账户增加、删除、权限分配；
c) 数据库管理，包括但不限于创建、删除、修改、备份和恢复。

7.6.3 日志保存

日志保存应符合以下要求：

a) 管理员应制定日志文件命名规则，并按照日志文件命名规则创建所需的日志文件；
b) 数据库管理员应防止日志数据丢失，要求日志存储已满时，应采取相应的防止日志数据丢失的措施，如：忽略审计事件、覆盖已存储的最久的审计事件、日志文件自动生长、重新创建日志文件等；
c) 日志文件应与数据库数据一样，定期备份并妥善安全保存这些备份日志，防止备份日志的丢失、泄露与被篡改。

7.6.4 日志访问

数据库管理员应采取措施保证只有授权用户才能访问日志信息。

7.6.5 安全审计

数据库管理员定期对数据库进行安全审计，内容包括但不限于：用户权限、访问限制。

7.7 网络数据库备份与恢复

7.7.1 总体要求

网络数据库备份与恢复应符合以下总体要求：

a) 数据库系统管理员应对数据库系统的配置参数及相关文件进行备份，当配置发生变更时必须编辑新的版本号且对变更前文件及变更后文件进行双重备份应制定数据库系统的备份策略，定期对数据库系统进行备份；
b) 数据库备份策略的制定应以高效备份与恢复为目标，并且能够与操作系统备份较好的结合，宜采用物理备份与逻辑备份相结合；
c) 对备份权限的设置加以严格控制；
d) 妥善存放和保管备份介质（包括磁带、从数据库导出的文件等），防止非法访问。对备份的介质应做好标识，存放环境符合要求；
e) 为防止数据篡改，保持数据的原始性，核心数据应有冷备份。

7.7.2 备份方式及策略

备份方式及策略应符合以下要求：

a) 完全备份：对备份的内容进行整体备份；
b) 增量备份：仅备份相对于上一次备份后新增加和修改过的数据；
c) 差异备份：仅备份相对于上一次完全备份之后新增加和修改过的数据；
d) 按需备份：仅备份应用系统需要的部分数据；
e) 根据各个应用能接受的恢复时间去选择对系统和数据的备份方式，并采取相应的备份策略；
f) 结合使用在线备份、逻辑备份和物理备份等多种方式，并且自动方式和手动方式相结合；
g) 数据备份应根据系统情况和备份内容，采用不同的备份方式及策略，并做好记录。

7.7.3 备份要求

备份应符合以下要求：

a) 为确保所备份的内容可再现系统的运行环境，数据备份内容应包括生产、管理等应用系统中的所有关键业务数据；
b) 对计算机和设备进行软件安装、系统升级或更改配置时，应进行系统和数据、设备参数的完全备份；
c) 对数据库的数据要求定时自动备份；
d) 建立备份文件档案及档案库，详细记录备份数据的信息；要做好数据备份的文卷管理，所有备份应有明确标识，包括卷包、运行环境、备份人；卷名应按统一的规则来命名；
e) 存档数据的保存时间可根据数据重要程度和有效利用周期确定；
f) 考虑备份介质的安全问题，既要保证存放的物理环境，也要避免对备份数据的非授权访问；
g) 数据备份应保存两份拷贝，一份在现办公地址保存，以保证数据的正常快速恢复和数据查询，另一份在现办公地址外保存，避免灾难后数据无法恢复；
h) 系统管理员和数据库管理员确定备份策略，由备份管理员执行备份。

7.7.4 恢复的管理

7.7.4.1 故障确认

故障确认应符合以下要求：

a) 在进行恢复之前，首先应确认造成故障的原因；
b) 应区分是操作系统的故障还是数据库的故障；
c) 应由系统管理员或数据库管理员负责，在完成故障分析后确认需要进行恢复操作时，由相应的管理者提交书面的故障分析报告。

7.7.4.2 制定恢复计划

备份系统管理员在收到故障分析报告后应与相应管理者一起制定详细的恢复计划，包括应恢复的内容、恢复的时间、恢复的操作步骤、恢复对应用造成的影响等，并形成书面的恢复计划。

7.7.4.3 恢复操作

恢复操作应符合以下要求：

a) 在进行实际恢复前，备份系统管理者与相应管理者应再次确认恢复计划的可行性及造成的后果；
b) 确认无误后进入到实际的恢复操作。在进行恢复前，现有的内容作相应的备份，以防止在恢复的过程中发生更进一步的错误；
c) 进行恢复操作时应将每一步的执行过程记录下来，以备后用。

7.7.4.4 恢复后的操作

数据恢复后，必须进行测试、验证、确认，确保数据恢复的完整性和可用性。在完成恢复结果测试成功后，对恢复后的系统进行相应的备份。最后，将执行恢复操作的管理者、恢复操作的时间、过程、完成的状况等形成书面报告。

7.7.5 对长期保存的备份进行校验

对长期保存的备份进行校验应符合以下要求：

a) 应每年对长期保存的备份进行校验，以防止需要时备份不可用的情况发生；
b) 应使用专业的校验工具进行。

7.7.6 异地容灾备份

异地容灾备份应符合以下要求：

a) 重要数据应设计和实施异地容灾方案，以防备不可预见的灾难对在线数据及其备份数据毁灭性的破坏；
b) 异地容灾备份的方式和频率要结合对数据的完全恢复或不完全恢复等因素进行考虑；
c) 异地容灾点应至少具备同区域异地备份点以及不同区域异地备份点两个以上。

7.8 网络安全防护

7.8.1 网络安全拓扑和分区设计

网络安全拓扑和分区设计应遵循合理分区原则，各个区域应物理隔离，并合理设置权限和配置防护措施。分区包括但不限于：

a) 互联网接入区；
b) 核心交换区；
c) 安全区；
d) 研发测试区；
e) 生产区；
f) 备份区；
g) 异地备份区。

7.8.2 网络安全设备保障

网络安全设备保障包括但不限于：

a) 防火墙：隔离内外网，是互联网与内网之间的一道屏障；
b) 入侵检测与自动防御系统：检测并处理各种网络安全攻击行为；
c) Web 应用防火墙：在应用层面保证了数据资源的安全性；
d) 堡垒机：运维人员使用的工具，包括分配权限、日志记录、审计等功能；
e) 防病毒网关：保证服务器终端防病毒安全。

参 考 文 献

[1] GB/T 25069—2010 信息安全技术 术语
[2] GB/T 31075—2014 科技平台 通用术语
[3] 贺桂英;周杰;王旅.数据库安全技术[M]，人民邮电出版社,2018
[4] 王瑞民.大数据安全技术与管理[M]，机械工业出版社,2021
[5] Ling Liu, M. Tamer Özsu; Encyclopedia of Database Systems[M]. Living reference work,2020
[6] 中华人民共和国数据安全法