ICS 35.240
CCS L70

团　体　标　准

T/CESA 1216—2022

计算机基本输入输出系统（BIOS）技术要求 第 2 部分：服务器

Technical requirement for computer basic input output system(BIOS)

Part 2： Server

2022-07-21 发布　　2022-08-20 实施

中国电子工业标准化技术协会　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。

本文件由中国电子技术标准化研究院提出并归口。

本文件起草单位：中国电子技术标准化研究院，华为技术有限公司、天津飞腾信息技术有限公司、龙芯中科技术股份有限公司、上海兆芯集成电路有限公司、无锡先进技术研究院、中电科技（北京）有限公司、南京百敖软件股份有限公司、阿里巴巴技术有限公司、统信软件技术有限公司、同方股份有限公司、腾讯科技(深圳)有限公司、浪潮电子信息产业股份有限公司、系微软件科技（上海）有限公司、海光信息技术股份有限公司、中国长城科技集团股份有限公司。

本文件主要起草人：李雪莲、钟伟军、任翔、赵鑫、宋博伟、齐筱、宋东匡、沈莉梅、聂永丰、刘勇鹏、舒奕棋、李超、李强、刘景龙、牛彦奎、苏卫强、沈金祥、陈小春 任彤、吴平、曹胜明、李羿、常琳、张磊、占俊、耿成山、杨蔚才、李志高、蒋增增、张炳会、李道童、樊青松、何治平、黎建根 成联国。

计算机基本输入输出系统（BIOS）技术要求 第2部分：服务器

1 范围

本文件规定了服务器BIOS的设备支持、一般功能、接口、安全、能效、可靠性与可用性以及人机配置界面要求。

本文件适用于服务器的设计和选型。

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。

高级配置与电源管理接口规范（ACPI Specification Version 6.3）

智能平台管理接口规范（IPMI Spefification V2.0 ）

DSP0266 Redfish规范 （Redfish Specification Version 1.11.0）

系统管理输入输出系统规范（SMBIOS Reference Specification, Version 3.3.0 ）

统一可扩展固件接规范（UEFI Specification Version 2.8）

3 术语和定义

下列术语和定义适用于本文件。

3.1

固件 firmware

固化到计算机中的非易失性存储器中的一组程序或软件。

3.2

基本输入/输出系统 basic input/output system

存于计算机主板上的固件，负责计算机开机时的硬件检测和初始化、操作系统安装和引导，并向操作系统提供计算机主板信息和服务接口。

3.3

统一可扩展固件接口 unified extensible firmware interface

操作系统和固件之间的接口，当前应用最广泛的一种 BIOS 固件接口标准。

3.4

基板管理控制器 baseboard management controller

部署于服务器主板上的具有独立供电、独立处理器、独立 I/O 接口的控制单元。

3.5

热键 hot key

BIOS 启动过程中能够响应的特定功能按键。

3.6

安全启动根 root of secure boot

安全启动的起点，是安全启动第一个被执行的程序，从它开始建立安全启动的可信链，保证整个

系统安全。

4 缩略语

下列缩略语适用于本文件。

ACPI：高级配置与电源管理接口（Advanced Configuration and Power Interface）

BIOS：基本输入输出系统（Basic Input Output System）

BMC：基板管理控制器（Baseboard Management Controller）

CPU：中央处理单元（Central Processing Unit）

ECC：错误检查和纠正技术（Error Checking and Correcting）

HDD：机械硬盘 （Hard Disk Drive）

HTTPS：安全超文本传输协议（Hypertext Transfer Protocol Secure）

IPMI：智能平台管理接口（Intelligent Platform Management Interface）

JEDEC：联合电子设备工程委员会 （Joint Electron Device Engineering Council）

KB：千字节 （Kilobyte）

OS：操作系统（Operating System）

PXE：预加载执行环境（Preboot eXecution Environment）

SMBIOS：系统管理基本输入/输出系统（System Management BIOS）

SPD：串行存在检测 （Serial Presence Detect）

SPI：串行外接口（Serial Peripherial Interface）

SSD：固态硬盘 （Solid State Drive）

TCM：可信加密模块（Trusted Cryptography Module）

UEFI：统一可扩展固件接口（Unified Extensible Firmware Interface）

USB：通用串行总线（Universal Serial Bus）

5 分级说明

根据BIOS技术发展阶段及技术要求必要性,本文件将BIOS技术要求划分为第一级别和第二级别。

第一级别：是BIOS的基本技术要求，规定服务器 BIOS 的基本能力（Level1）。

第二级别：是BIOS的高级或扩展要求，体现服务器 BIOS 的发展方向，满足用户对服务器 BIOS 更高的技术需求（level2）。

6 设备支持

6.1 处理器支持

本规范适用于ARM、X86、MIPS、SunWay等处理器架构。

6.2 内存支持

BIOS能正确的识别和初始化处理器所能支持的内存模组类型。（Level1）

BIOS对内存的初始化应基于JEDEC规范定义的SPD数据，SPD数据来源可以从内存模组读取，也可以按SPD格式在代码中预设，以支持颗粒形式的内存。（Level1）

内存工作频率默认初始化成CPU、内存共同支持且不高于BIOS配置界面设置的最高频率。（Level1）

6.3 BIOS Flash芯片支持

BIOS 能正确的识别和初始化不同总线协议的 Flash 芯片，例如 SPI Flash。（Level1）

6.4 存储设备支持

BIOS 对于存储设备的支持主要包括以下要求:

a) BIOS 能正确识别和初始化不同接口或不同总线协议的存储设备，至少应支持 SAS、SATA、PCIe 接口的 HDD 或 SSD。（Level1）
b) BIOS 能从源存储设备将操作系统安装至目标存储设备中。例如，可通过光驱、闪存盘安装操作系统到目标硬盘。（Level1）

6.5 输入输出设备支持

BIOS 对于输入输出设备的支持主要包括以下要求:

a) BIOS 支持 USB 键盘。（Level1）
b) 在硬件和平台支持的情况下，BIOS 能支持串口和 VGA 控制台输出。（Level1）

6.6 板卡支持

BIOS 对于板卡的支持主要包括以下要求:

a) BIOS 能正确地识别常见的 PCIe 板卡，包括网卡、RAID 卡和显卡等。（Level1）
b) BIOS 应对板卡进行正确的识别和基本的资源分配，使其在操作系统阶段具备相应的功能。（Level1）
c) 在存在相应 CPU 指令集的板卡 UEFI 驱动时，BIOS 应能加载并运行相应 UEFI 驱动，在开启安全启动时，只有通过签名校验的板卡 UEFI 驱动才能被运行。（level2）

6.7 BMC 支持（适用时）

BIOS 对于 BMC 的支持主要包括以下要求:

a) 当计算机使用 BMC 中的显示或串口设备作为主机系统的显示或串口设备时，BIOS 能正确的初始化 BMC 中的显示和串口，使其在 BIOS 下具备相应的功能。（Level1）
b) BIOS 能识别和初始化 BMC 端远程挂载的虚拟输入设备（键盘、鼠标）。（Level1）
c) BIOS 能识别和初始化 BMC 端远程挂载的虚拟媒体设备。（Level1）
d) 初始化 BIOS 和 BMC 通信接口，通信协议符合 IPMI 或 Redfish 规范。（Level1）

7 一般功能

7.1 启动操作系统

在启动操作系统过程中，BIOS 应满足以下要求:

a) BIOS 加载启动操作系统的方式符合 UEFI 规范定义。（Level1）
b) BIOS 按启动项的先后顺序依次尝试启动项，完成操作系统启动。（Level1）

7.2 文件系统支持

BIOS 应支持 UEFI 规范定义支持的文件系统。（Level1）

7.3 BIOS 升级

BIOS 升级方式和升级要求应满足以下指标的规定:

a) BIOS 升级包括带内升级和带外升级两种方式。带内升级宜在操作系统下执行，带外升级宜由

BMC 负责，由相应 BMC 规范进行约定。带内升级和带外升级支持其一即可。（Level1）

b) BIOS 升级应符合以下要求：

1) BIOS 升级之前应有醒目提示信息，提示用户切勿断电或重启机器。（Level1）
2) BIOS 开始升级之后到升级完成应无需人工干预。（Level1）
3) BIOS 升级过程应有进度显示，如百分比。（Level1）
4) BIOS 升级完成之后应重启后生效。（Level1）
5) 默认情况下，经用户设置的 BIOS 配置在 BIOS 升级后保持不变，升级前后版本不兼容时可例外。（Level1）
6) BIOS 升级应具备签名校验功能，只有目标镜像签名校验通过之后才能进行升级。(Level2)

c) 采用带内安全升级且开启 BIOS 代码区域保护时，最终更新 BIOS 的操作应在 BIOS 下完成。（Level2）

7.4 网络引导

BIOS 应满足以下网络引导的类型和要求:

a) BIOS 支持标准的 PXE 引导，CPU 类型定义应符合 RFC5970 3.3.Client System Architecture Type Option 规范定义，如 X86、ARM、ARM64、RISC-V、龙芯、申威等。（Level1）
b) BIOS 支持 HTTPS boot。（Level2）

7.5 诊断功能

为了在系统发生故障时能够快速定位故障位置和故障原因，BIOS 应具备必要的诊断功能:

a) 诊断信息输出方式至少包含下面其中一种：

1) 调试端口
BIOS 在运行过程中的关键点输出到特定调试端口。（Level1）
2) 串口日志
BIOS 在运行过程中将重要的日志信息以文本形式输出到串口。（Level1）
3) 内存日志
BIOS 在运行过程中将重要的日志信息以文本方式输出到内存，并能将内存中日志信息保存到非易失存储设备中或传递给 BMC 或传递给操作系统。（Level1）

b) 应记录的诊断信息包括但不限于：

1) 检测到无内存设备；（level2）
2) 内存初始化成功或失败；（Level1）
3) 检测到无显示输出设备；（level2）
4) 检测到无启动设备。（level2）

7.6 电源管理

在硬件平台支持的情况下，BIOS 应支持 ACPI 电源管理模式中的 S0、S5 模式。（Level1）

7.7 主板管理

在计算机具备 BMC 的情况下，用户可以通过 BMC 对主机系统进行一些带外管理操作，BIOS 要求能支持这些带外管理功能：

a) BIOS 支持从 BMC 端的远程媒体挂载设备进行操作系统的安装。（Level1）
b) BIOS 支持 BMC 端进行设备启动顺序的修改。（Level1）

8 接口

8.1 SMBIOS

BIOS 应向操作系统或应用提供 SMBIOS 规范定义的常规表格接口，以便操作系统或应用能通过 SMBIOS 表格获取硬件平台的一些基本信息。（Level1）

8.2 ACPI

在硬件平台支持 ACPI 规范的情况下，BIOS 应向操作系统或应用提供常规的 ACPI 表格和配置方法接口，以便操作系统或应用能通过 ACPI 表格和配置方法接口来实现对主机的一些高级配置功能和电源管理功能。（Level2）

8.3 内存映射

BIOS 应向操作系统提供系统的内存布局和内存属性等信息，满足 UEFI 规范定义。（Level1）

BIOS 提供的内存映射信息中操作系统运行阶段需保留的内存应满足按内存属性 64KiB 对齐，即同一个 64KiB 地址空间内只有一种内存属性，使操作系统可以使用 64KiB 或 4KiB 的页表。（Level2）

8.4 运行时服务

BIOS 能向操作系统或应用提供 UEFI 规范中描述的运行时服务（Runtime Service）函数接口。基本运行时服务应包括 GetTime/SetTime、GetVariable/SetVariable、ResetSystem 等。（Level1）

9 安全

9.1 BIOS 口令功能

BIOS 口令应满足以下要求:

a) BIOS 支持管理员密码和普通用户密码两种密码，两种密码相互独立，普通用户密码由管理员进入 BIOS 配置界面设置，在使用者无需求的情况下，亦可不设置。（Level1）

b) 如果设置了密码，使用者进入 BIOS 配置界面需要进行密码验证，只有验证成功后才能进行功能配置和信息查询等操作，采用管理员密码验证通过时被确认为管理员操作，采用普通用户密码验证通过时被确认为普通用户操作。（Level1）

c) 管理员具有修改 BIOS 配置界面所有可改选项的权限，包括设置、修改和清除普通用户密码。

d) 普通用户可以查看 BIOS 配置选项，可以修改但不可清除普通用户密码。（Level1）

e) 支持对密码进行复杂度校验，避免使用者设置过于简单的密码，当设置的密码不符合要求时应提示用户不符合的原因。密码复杂度要求为：（Level2）

   （1）密码长度至少 8 个字符；

   （2）至少包含以下 4 种字符中的 2 种 ：

      a) 特殊字符：`~!@#$%^&*()-_=+\|[{}];:'",<.>/?和空格；

      b) 小写字母：a ～ z；

      c) 大写字母：A ～ Z；

      d) 数字：0 ～ 9.

f) 管理员密码和普通用户密码不应以明文方式存储。（Level1）

g) 新设置的管理员密码与历史管理员密码至少 3 次不重复，对普通用户密码无要求。（Level2）

h) 出厂禁止存在缺省密码，采用“首次登录设置”模式，首次登录必须强制设置管理员密码。（Level2）

i） 密码支持防暴力破解，使用者每次密码操作应进行日志记录，如果连续 3 次以上登录失败应告警并锁定，锁定后，可等待超时解锁或者重启系统才能进行再次操作，单次超时解锁时间不少于 3 分钟。（Level2）

9.2 安全启动

安全启动的作用是检测设备启动阶段固件以及软件是否被篡改，保护设备启动阶段的完整性。BIOS 对安全启动的支持应满足以下要求:

a） BIOS 启动过程中应对待运行的程序进行签名校验，只有认证通过才能被运行。（Level1）
b） BIOS 支持 UEFI 规范定义的 Secure Boot 功能。（Level1）
c） BIOS 配置界面中支持对第三方证书的注册、删除。（Level1）
d） 安全启动根应内置于 CPU 芯片内或第三方硬件内，且满足出厂固化、启动不可绕过、内容不可被外部读取、内容无法被篡改的要求。（Level2）
e） 管理员可以通过 BIOS 配置界面设置安全启动关闭或开启。（Level1）

9.3 可信度量（Level2）

BIOS 对可信度量的支持应满足以下要求:

a） BIOS 在启动过程中自动识别和初始化可信模块。（Level1）
b） 在可信模块可用的情况下，BIOS 应向操作系统报告可信模块信息。（Level1）
c） 在可信模块可用的情况下，BIOS 启动过程中，为关键部件进行度量，并将结果存入可信模块，同时记录度量事件，支撑建立信任链。（Level1）
d） BIOS 管理员配置界面支持可信模块的可用性配置。（Level1）

9.4 密码算法强度

BIOS 安全启动校验、安全升级和用户密码认证都会使用到密码算法:

a） 禁止使用私有的、非标准的密码算法。（Level1）
b） 哈希、签名算法需满足安全强度以及对应生存周期要求，应采用如下推荐算法或同等强度的算法，见表 1：（Level1）

注：“同等强度的算法”指由算法采用者举证该算法具备与推荐算法同等安全强度，下同。

表 1 算法安全强度对应生存周期要求

用途	推荐算法
哈希计算	SHA256 或以上 SM3
非对称加密	RSA (≥2048 bits) SM2
数字签名	RSA(≥2048 bits) ECDSA(≥256 bits) SM2 SM3

9.5 BIOS 密码加密算法

BIOS 对密码加密算法的支持应满足以下要求：

a) 存储 BIOS 密码时，应采用加盐加密算法，宜使用 PBKDF2 或 scrypt 算法，或具备同等强度的算法加密存储。（Level1）

b) BIOS 密码做单向不可逆加密时，迭代次数缺省宜设为 10000 次，对于有性能约束的产品，迭代次数至少 1000 次。（Level1）

c) 应确保不同用户使用不同盐值，盐值 salt 的长度至少 8 字节，且应满足本规范中随机数要求。（Level1）

9.6 密码算法中使用到的随机数

硬件支持真随机数的情况下，应采用真随机数，硬件不支持真随机数的情况下，可采用伪随机数：

a) 伪随机数应由密码学安全伪随机数生成器（CSPRNG）生成，如 OpenSSL 的 rand 库函数。（Level1）

b) 真随机数应由真随机数发生器（TRNG）生成。（Level2）

9.7 BIOS 代码区域保护

在硬件支持的情况下，要求系统运行时对 BIOS 代码所在的 CPU 和内存以外的存储区域进行写保护，防止 OS 下恶意软件破坏 BIOS 代码。（Level2）

9.8 敏感信息处理

内存中的敏感信息使用完毕后应及时清除，并不可通过任何手段恢复，包括但不限于密码、密钥。（Level1）

10 能效要求

10.1 支持 CPU 调频功能

在硬件支持的情况下，BIOS 支持 CPU 调频功能，按照 ACPI 规范给操作系统提供 CPU 调频功能接口。（Level2）

10.2 支持 CPU 休眠功能

在硬件支持的情况下，BIOS 支持 CPU 中部分核休眠唤醒功能，按照 ACPI 规范提供休眠唤醒功能接口给操作系统。（Level2）

10.3 支持功耗封顶功能

在硬件支持的情况下，BIOS 可以接受带外或带内下发的功耗封顶要求，对单板实施功耗控制，达到实际功耗不超过目标功耗的效果。（Level2）

11 故障处理能力

11.1 支持硬件故障处理与上报功能

BIOS 对硬件故障处理与上报的支持应满足以下要求：

a) 系统硬件发生故障并触发中断信号时，BIOS 应首先响应并进行处理，故障处理不限于故障恢复、故障隔离、故障上报等可以降低故障影响、有利于提高系统可靠性、可用性的措施；（Level2）

b) BIOS 应向 OS 报告故障信息，信息内容满足 ACPI 规范中 APEI（ACPI Platform Error Interfaces）要求；（Level2）
c) 在具备 BMC 的系统中，BIOS 同样应将故障信息报告给 BMC，信息格式由 BIOS 与 BMC 自行约定。（Level2）

11.2 支持启动阶段故障核隔离功能

BIOS 对启动阶段故障核隔离的支持应满足以下要求：
a) 当启动阶段故障核隔离功能开启时，BIOS 启动过程中，如果检测到会导致 CPU 核无法工作的故障，例如 CPU 核对应的 cache 故障，则 BIOS 应将该故障核隔离，使其不再工作，其他正常核工作不受影响。（Level2）
b) 在隔离故障核时，BIOS 应更新 ACPI 表，为 OS 屏蔽故障核信息，避免 OS 因使用故障核而发生异常。（Level2）
c) 如果故障核为 BIOS 启动所用的核，那么不适用此条规则。（Level2）
d) BIOS 可通过配置界面控制核故障隔离功能的开启和关闭。（Level2）

11.3 支持内存 ECC 功能

BIOS 应支持带 ECC 功能的内存条。（Level1）

11.4 支持初始化阶段内存故障隔离

BIOS 对初始化阶段内存故障隔离的支持应满足以下要求：
a) 当初始化阶段内存故障隔离功能开启时，在 BIOS 执行内存初始化阶段，发现内存无法通过初始化或无法通过测试时，BIOS 应根据内存错误情况对相关 rank、DIMM 或者 channel 进行隔离，如果隔离之后还有可用内存，则继续完成系统启动。（Level1）
b) Rank、DIMM、channel 隔离采用最小代价原则，即隔离优先级排序为 Rank、DIMM、channel。（Level1）
c) BIOS 可通过配置界面控制初始化阶段内存故障隔离功能的开启和关闭。（Level1）

12 人机配置界面

12.1 支持热键操作

BIOS 应支持通过热键执行相应功能，热键功能应包含进入配置界面、进入启动项管理界面、执行网络引导。（Level1）

12.2 BIOS 配置界面

BIOS 配置界面的规格应满足以下要求：
a) 配置界面应能显示系统的基本信息，包括但不限于 BIOS 信息、主板信息、处理器信息、内存信息、日期时间信息等。（Level1）
b) 配置界面显示语言支持中文汉字或者英文，如果同时支持，则可在配置界面进行设置。（Level1）
c) 在硬件支持的情况下，应支持如下功能：（Level1）
    1) 内存配置：支持最大内存频率配置，支持内存交织模式配置，支持内存 NUMA 开关配置。

2) 虚拟化配置：支持 SR-IOV 开关配置。
3) 端口开关配置：支持各端口单独开关配置。
4) 网络配置：支持 PXE 开关配置。

d) 在有 BMC 的情况下，支持 BMC 版本号的显示，支持 BMC IP 的显示和配置。（Level1）
e) 在有看门狗的情况下，支持看门狗配置，包含看门狗开关配置，超时时间配置，超时后执行策略配置。（Level1）
f) 配置界面应提供 BIOS 密码的设置、修改和清除功能。（Level1）
g) 配置界面应提供启动项优先级的配置功能。（Level1）
h) 配置界面应提供恢复默认配置功能。（Level1）