ICS 35. xxx
CCS Lxx

团 体 标 准

T/ISC XXX—XXXX

安全可信中间件能力要求 第 4 部分 应用服务器中间件

Requirements for Secure and Trustworthy Middleware Capability Requirements
Part 4:Application Server Middleware

xxxx－xx－xx 发布 xxxx－xx－xx 实施

中 国 互 联 网 协 会 发布

目次

前　　言 II
引　　言 III
安全可信中间件能力要求 第4部分 应用服务器中间件 1
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
3.1 中间件 middleware 1
3.2 事件监听器 Event Listener 1
3.3 过滤器 Filter 1
3.4 处理XML的Java接口 Java API for XML Processing 2
3.5 Java 消息服务 Java Messaging Service 2
3.6 Java 名字和目录服务接口 Java Naming and Directory Interface 2
4 符号和缩略语 2
5 安全可信要求 2
6 应用服务器中间件能力要求 3
6.1 功能要求 3
6.2 性能要求 7
6.3 可靠性要求 7
6.4 安全性要求 7
6.5 可维护性要求 8
6.6 可扩展性要求 9
6.7 兼容性要求 9

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。

本文件由中国互联网协会提出并归口。

本文件起草单位：

本文件主要起草人：

——

引　言

随着信息技术的快速发展和数字化转型的深入推进，中间件技术作为软件基础设施的重要组成部分，正被广泛应用于互联网、金融、通信、交通、医疗等多个关键领域，显著提升系统间通信效率，降低系统耦合度，增强数据处理能力，有效提升信息系统的整体性能与稳定性。

安全可信中间件往往基于自主研发的软硬件基础设施，具备高度的自主性与良好的兼容性，能够在复杂的系统环境中平稳运行。尤其针对党政、医疗、金融等对数据安全和系统可靠性要求严苛的行业，安全可信中间件提供了有效的数据安全保障机制，能够防范外部恶意攻击，保障数据的机密性、完整性和可用性，对推动重点行业的数字化转型和保障关键领域信息安全具有重要意义。

本系列标准针对中间件产品研发和行业用户应用过程中所面临的安全风险与挑战，依据现行法律法规和行业特定需求，明确安全可信中间件的技术要求和可信验证机制，建立涵盖基础环境适配、软硬件设施建设、平台功能开发的统一标准体系，规范产品研发、应用部署和服务保障等全生命周期管理活动。通过构建科学合理的安全可信体系指引和产品能力量化评估标准，为产业发展提供有力的技术支撑，促进市场可持续健康发展。本文件针对安全可信应用服务器中间件能力要求进行规范。

对本文件中的具体事项，法律法规另有规定的，需遵照其规定执行。

安全可信中间件能力要求 第4部分 应用服务器中间件

1 范围

本文件规定了应用服务器中间件的功能要求、性能要求、可靠性要求、安全性要求、可维护性要求、可扩展性要求和兼容性要求。

本文件适用于从事安全可信应用服务器中间件研发、应用及评价的各类机构。

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 33847—2017 信息技术 中间件术语

GB/T 28168-2025 信息技术 中间件 消息中间件技术要求

GB/T 26232—2025 基于J2EE的应用服务器技术规范

3 术语和定义

GB/T 33847—2017、GB/T 28168—2025、GB/T 26232-2025界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了GB/T 33847—2017、GB/T 28168—2025、GB/T 26232-2025中的某些术语和定义。

3.1

中间件 middleware

位于系统软件之上,用于支持分布式应用软件,连接不同软件实体的支撑软件（2.1）。

[来源：GB/T 33847—2017，2.1]

3.2

事件监听器 Event Listener

Servlet 规范中规定的，可以对 Servlet 上下文、HTTP 会话或 Servlet 请求的事件通知进行监听处理的代码组件。

[来源：GB/T 26232—2025，3.1.3]

3.3

过滤器 Filter

Servlet 中的过滤器 Filter 是实现了 javax.servlet.Filter 接口的服务器端程序，能够转换网络 请求、应答、头部中内容，并做一些业务逻辑判断等。

[来源：GB/T 26232—2025，3.1.5]

3.4

处理 XML 的 Java 接口　Java API for XML Processing

一种支持 XML 文档处理的 Java API，用于 XML 文档解析和转换。

[来源：GB/T 26232—2025，3.1.13]

3.5

Java 消息服务　Java Messaging Service

基于点到点或者发布订阅的交互方式来支持应用程序之间的异步通讯的消息服务。

[来源：GB/T 26232—2025，3.1.11]

3.6

Java 名字和目录服务接口　Java Naming and Directory Interface

Java 中使用命名和目录服务接口，包含应用层访问接口和服务提供者接口。

[来源：GB/T 26232—2025，3.1.12]

4　符号和缩略语

下列符号和缩略语适用于本文件。

API：应用编程接口（Application Programming Interface）

EJB：基于分布式事务处理的企业级应用（Enterprise JavaBean）

HTML：超文本置标语言（Hyper Text Markup Language）

HTTP：超文本传输协议（Hypertext Transfer Protocol）

HTTPS：基于SSL的超文本传输协议（Hypertext Transfer Protocol over SSL）

ID：身份（Identity）

JAAS：Java 认证和授权服务（Java Authentication and Authorization Service）

JavaEE：Java 企业版（Java Enterprise Edition）

JCA：Java 连接器架构（Java EE Connector Architecture）

JDBC：Java 数据库连接（Java Database Connectivity）

JMS：Java 消息服务（Java Message Service）

JMX：Java 管理扩展（Java Management Extensions）

JNDI：Java 名字和目录服务接口（Java Naming and Directory Interface）

JPA：Java 持久化API（Java Persistence API）

JSP：Java 服务器端页面（Java Server Pages）

JVM：Java 虚拟机（Java Virtual Machine）

SOAP：简单对象访问协议（Simple Object Access Protocol）

SSL：安全套接层（Secure Sockets Layer）

StAX：XML 流式接口（Streaming API for XML）

XML：可扩展置标语言（Extensible Markup Language）

5　安全可信要求

安全可信要求须符合《安全可信中间件能力要求 第1部分 总体要求》中5的规定。

6 应用服务器中间件能力要求

6.1 功能要求

6.1.1 安装部署

应用服务器的的安装部署应符合国家标准GB/T26232-2025中14.1的全部要求。为便于实施，现将核心条款摘要如下：

a） 应用服务器中间件可提供图形界面形式的安装和卸载程序,引导用户安装和卸载的全过程。
b） 应用服务器中间件的安装和卸载不影响其他应用程序的正常运行。
c） 应用服务器中间件应提供命令行方式启动和停止应用服务器中间件。

6.1.2 交互

a） 应确保与业务系统之间的数据交换的一致性，并遵循标准化接口。
b） 应支持多节点部署，能够实现负载均衡。
c） 应提供数据加密功能。
d） 应通过标准协议提供消息队列功能。
e） 应支持分布式事务，确保跨服务操作的原子性、一致性、隔离性等特性。
f） 应实现缓存机制。
g） 应支持限流与熔断功能。
h） 应支持连接池、线程池等资源管理。

6.1.3 集成

a） 应支持根据任务优先级进行调度，确保关键任务优先执行，提升整体效率和响应速度。
b） 应具备容错机制，支持任务失败时自动恢复或重新调度。
c） 应支持多种通信协议，确保不同系统间有效通信，同时实现安全的数据传输和故障恢复机制。
d） 应支持跨多个系统和数据库的事务管理，确保事务的 ACID 属性（原子性、一致性、隔离性和持久性）。
e） 应支持模块化和组件化设计，允许应用程序独立服务，便于集成和替换。
f） 应支持微服务架构和异步消息传递，促进应用程序解耦并提升灵活性。
g） 应提供部署、管理和监控工具，简化应用程序的生命周期管理并实时监控其性能。
h） 应支持蓝绿发布、金丝雀发布等模式，确保应用版本更新过程中的平稳过渡与最小化风险。
i） 应支持容器化部署和云原生技术，实现快速部署与扩展。
j） 应兼容服务网格架构进行流量治理，并提供 API 网关集成功能，支持鉴权、限流与熔断管理。

6.1.4 配置与管理

a） 应支持用户的添加、编辑和删除，并提供内置用户管理系统，包括认证、授权和操作审计功能。
b） 应支持对容器资源进行编排管理，确保资源的高效利用与调度。
c） 应提供服务器开发与维护的必要控制，并提供生命周期定义文档，明确开发和维护模型。
d） 应支持对配置的批量管理，如批量备份和还原等。
e） 应支持全局配置在线管理，能够查看和修改配置参数，确保配置的一致性。
f） 应支持使用配置管理系统对所有配置项进行维护，并进行唯一标识。
g） 应提供配置管理文档,描述如何唯一标识和管理配置项,包括配置管理计划和开发实施一致性。
h） 应配置管理系统提供自动化支持，确保配置项仅接受授权变更。

i） 应支持命令行方式进行参数配置管理，简化操作和控制。
j） 应涵盖服务器本身、其组成部分的配置管理。

6.1.5 运维

a） 应定期巡检平台功能，确保系统各项功能正常运行。
b） 应提供运维辅助功能，提升运维效率和系统可靠性。
c） 应支持故障迁移、故障修复等功能，并能够与智能运维系统集成。
d） 应支持自动化部署、配置管理、更新和回滚等功能，简化运维过程。
e） 应提供自动化工具或脚本，自动进行巡检，包括系统配置、资源利用和性能指标的检查。

6.1.6 Web 容器

6.1.6.1 Servlet 容器

a） 应遵守Servlet4.0或以上规范，并宜支持Servlet5.0。
b） 应支持实现javax.servlet.Servlet接口的servlet组件，并确保严格遵守Servlet生存周期，包括加载、实例化、初始化、处理请求和终止服务。
c） 应支持容器启动时或延迟初始化时加载和实例化Servlet，并通过Java类加载机制加载Servlet类。
d） 应支持在处理客户端请求前初始化Servlet，并允许进行资源初始化及一次性任务处理。
e） 应通过ServletRequest和ServletResponse对象处理请求和响应，并支持HTTP协议升级机制。
f） 应支持在需要时移除Servlet实例并支持Servlet的循环使用。
g） 应支持Servlet3.1或以上规定的过滤器功能，包括自定义过滤器的创建、配置和生命周期管理。
h） 应支持会话追踪和存储，符合相关标准，并宜支持分布式缓存或内存网格存储会话。
i） 应支持Web应用中的注解（如@WebServlet、@WebFilter等）和Web模块、共享库、JSP组件的可插拔性。
j） 应支持各种Servlet事件监听器（如ServletContextListener、HttpSessionListener等），并在相关事件发生时通知注册的监听器。
k） 应支持HTTP异常和Servlet异常处理，通过web.xml配置异常页面，处理HTTP状态码或Servlet异常。

6.1.6.2 JSP 组件支持

a） 应遵守Servlet3.1或以上规范，并宜支持Servlet4.0或以上规范。
b） 应支持实现javax.servlet.Servlet接口的servlet组件，并确保严格遵守Servlet生存周期，包括加载、实例化、初始化、处理请求和终止服务。
c） 应支持JSP2.3或以上的全部功能。
d） 应支持JSP组件的转化与编译，将JSP页面转化为Servlet类，并按照Servlet生存周期进行执行管理。
e） 应支持JSP2.1或以上规定的各种JSP元素类型的转换（动作、指令、表达式语言元素和脚本元素等）。

6.1.7 EJB 容器

a） 应支持EJB3.2或以上的全部功能，包括EJB定时器服务、拦截器、依赖注入、实例池和实例缓存等功能。
b） 应支持符合GB/T26232-2025中7.2.1.1的会话Bean规范。
c） 应支持符合GB/T26232-2025中7.2.1.2的消息驱动Bean规范。

d） 应支持定时器功能。
e） 应支持拦截器功能。
f） 应支持实例池机制。
g） 应支持实例缓存机制。
h） 应支持EJB文件标注。
i） 应支持依赖注入。
j） 应支持拦截器链配置。

6.1.8 连接服务

a） 应提供对HTTP1.0和1.1的支持，宜支持HTTP2.0。
b） 应支持HTTP配置功能。
c） 应支持HTTPS协议。
d） 应支持HTTPS配置功能。
e） 宜支持HTTPS访问控制。
f） 虚拟主机应符合GB/T26232-2025中6.1.3的规定。
g） 应支持与第三方Web服务器的集成，符合GB/T26232-2025中9.3的规定。

6.1.9 数据库连接服务

a） 应提供统一的数据库连接服务，屏蔽不同数据库的细节，确保平台无关性。
b） 应通过JDBC4.0或以上扩展API，支持本地事务和XA事务连接，并提供数据库连接池功能。
c） 应支持动态创建和删除数据库连接池。
d） 应支持动态修改连接池属性。
e） 应支持多数据源管理。
f） 应支持连接跟踪与超时提示。

6.1.10 持久化服务

a） 应支持JPA2.1或以上，提供实体对象/关系映射、查询处理和缓存功能。
b） 应为开发可伸缩、支持事务的程序提供运行环境，确保持久性实体的事务一致性。
c） 应将持久性实体与底层持久性细节隔离，开发者只需定义实体类，无需关注具体实现。

6.1.11 消息服务

a） 应支持JMS2.0或以上，并提供消息传递、事务型消息、一致性消息及持久订阅者支持，支持点对点和发布/订阅模式的消息生产与消费。
b） 应支持统一消息模型。
c） 应提供JMS连接工厂。
d） 应支持目的地对象。
e） 应支持标准JMS服务接入。
f） 应支持JNDI结构。
g） 应支持全局命名空间、应用命名空间、模块命名空间和组件命名空间。
h） 应支持JNDI命名服务的实现，提供对象的注册、查找、绑定、删除、重命名等功能。
i） 应支持JNDI配置方式。

6.1.12 邮件服务

a） 应具备向简单的应用程序添加电子邮件功能，适当的封装常用邮件功能和协议。
b） 应支持不同的消息传递系统实现消息存储、不同的消息格式和不同的消息传输。
c） 应提供了一组基类和接口，用于定义客户端应用程序的API。
d） 应用服务器应对JavaMail1.6或以上提供完整的支持。

6.1.13 连接器架构

a） 应支持在JCA容器中运行第三方的适配器，将JavaEE应用连接到任何应用系统或者资源。
b） 应支持JCA容器管理池化连接，安全上下文，XA事务。
c） 应支持外部系统使用端点来调用应用服务器内部的应用或者资源，实现与应用服务器的交互。

6.1.14 工作管理器

应提供对工作管理器的支持，允许应用程序通过工作管理器使用线程池中的线程来运行创建的工作任务。

6.1.15Web 服务

a） 应提供将普通Java类编译、打包、发布为Web服务的能力，宜提供相应的工具支持。
b） 应提供对Web服务组件的动态部署和管理功能。
c） 应支持WebSocket1.1协议。

6.1.16 参数配置规范

a） 应支持多种方式完成管理和配置，包括Web管理控制台、命令行工具以及HTTP接口。
b） 应支持灵活的功能模块配置，如JVM参数、Web容器参数、EJB容器参数等。

6.1.17 企业应用

a） 应支持EAR包封装。
b） 应支持资源适配器（连接器应用）。
c） 应支持Web方式管理工具。
d） 应支持动态监控功能。
e） 应提供日志管理、审计、查看、保存等功能。

6.1.18 接口规范

a） 应提供其他系统进行访问的接口，方便对应用服务器进行系统集成。
b） 应提供JMX接口和HTTP接口。

6.1.19 集群管理工具规范

a） 应支持Web应用集群部署。
b） 应支持会话管理。
c） 应提供请求转发功能。
d） 应支持亲合会话。
e） 应支持非亲合会话。
f） 应提供集群管理工具。

6.2 性能要求

a） 应保障业务通信和数据源通信的吞吐能力。
b） 应确保长时间运行的稳定性。
c） 应保障协作插件工具的响应时间。
d） 应保障管理平台的吞吐能力。
e） 应提供性能优化配置支持。

6.2.1 容量特性要求

a） 应使用压测工具进行性能压测，使CPU、内存其中之一系统资源达到100%，然后查看当前并发请求数
b） 应支持弹性扩展，可根据负载自动调整实例。

6.3 可靠性要求

6.3.1 基础能力

a） 应支持实例高可用性。
b） 应支持多操作系统。
c） 应支持大量并发连接。
d） 应支持定制。
e） 宜提供故障实例自动重启

6.3.2 自适应能力

a） 应支持流行开发框架。
b） 应兼容国外应用服务器。
c） 宜提供迁移工具

6.3.3 容错能力

a） 应支持节点故障时保证服务。
b） 应实现多种容错策略。
c） 应确保应用独立性。
d） 集群环境下单节点失效时仍能提供服务。

6.3.4 易恢复性

a） 应支持自动恢复服务。
b） 应保持会话信息。
c） 应支持数据源恢复。
d） 应保证事务一致性。

6.4 安全性要求

6.4.1 系统安全

a） 应隐藏软件版本和操作系统信息。
b） 应配置日志记录与监控系统。

c） 宜支持操作审计功能。

6.4.2 数据安全

a） 应支持传输加密。
b） 应支持数据访问鉴别。
c） 应支持数据完整性验证。
d） 应支持事务管理。

6.4.3 身份标识与鉴别

a） 应支持唯一身份标识和鉴别。
b） 应支持口令修改机制。
c） 应支持口令复杂度验证。
d） 应支持鉴别失败处理功能。
e） 应支持加密方式存储鉴别信息。

6.4.4 JAAS 安全框架

a） 应支持JAAS安全服务。
b） 应完全支持JAAS1.0或以上。
c） 应遵从JACC规范。
d） 应提供灵活的安全框架。

6.4.5 JavaEE 安全

a） 应支持声明式安全。
b） 应支持安全域管理。
c） 应支持安全上下文管理。
d） 应支持程序式安全API。
e） 应支持Web端安全认证。

6.5 可维护性要求

6.5.1 系统升级

a） 应支持系统增量升级功能，对系统部件、安全补丁等升级。
b） 应支持在线升级和离线升级，且升级不得修改破坏用户数据，不得影响原有软硬件兼容性。
c） 应支持升级回退机制，能卸载已升级的软件包，恢复系统原有状态。如升级为不可回退，则系统升级前以显式的提示告知用户。

6.5.2 监控告警

a） 应支持对代理目标的请求状态、客户端、请求数、平均响应时间等指标进行统计。
b） 应支持对上游节点的请求状态、客户端、请求数、平均响应时间等指标进行统计。
c） 应支持对虚拟主机的连接、请求状态、客户端占比等性能指标进行统计。
d） 应支持提供邮件、短信告警，支持导出告警信息。
e） 应支持提供添加、消除告警屏蔽。
f） 应支持设置和管理监控指标的阈值，当指标超过设定的阈值时触发告警通知。

g） 应支持提供告警分类、分级。
h） 宜支持告警抑制和降噪，避免相同问题重复告警。
i） 宜提供热更新能力，无需重启服务即可加载新配置或代码。

6.6 可扩展性要求

6.6.1 产品手册

产品手册的提供应符合GB/T26232-2025中15.1的规定。

6.6.2 帮助功能

帮助功能应符合GB/T26232-2025中15.2的规定。

6.6.3 应用示例

应用服务器应至少提供以下方面的具有说明的应用示例包：
a） JSP组件的使用。
b） Servlet组件的使用。
c） 无状态会话bean的使用。
d） 有状态会话bean的使用。
e） 数据库连接池的使用。

6.6.4 启动和停止

启动和停止应符合GB/T26232-2025中14.1的规定。

6.6.5 界面设计

界面设计应符合GB/T26232-2025中9.1的规定。
a） 应支持使用第三方语言扩展现有的产品能力。
b） 应支持Redis标准协议（RESP）以兼容现有客户端。
c） 应支持插件化架构，允许通过模块扩展新功能。
d） 宜支持计算和存储分离。

6.7 兼容性要求

a） 应基于安全可信CPU、操作系统、数据库等。
b） 应在所有应用平台上提供一致的应用开发接口，以实现应用程序在不同平台上的迁移。