ICS 35.240.01
CCS L 80

T/CUPC

团　　体　　标　　准

T/CUPC XXX-XXXX

零信任架构下的动态访问控制算法实施指南

Implementation guide for dynamic access control algorithms under zero trust architecture

（征求意见稿）

20XX-XX-XX 发布　　20XX-XX-XX 实施

中国城镇化促进会　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 总则 2
5 总体架构 2
6 算法输入因子规范 3
7 算法类型及实施技术要求 3
8 全流程实施规范 4
9 访问决策与会话管控 6
10 隐私安全要求 7
11 测试验证 7
12 运维与审计 8

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。

本文件由天津仁爱学院提出。

本文件由中国城镇化促进会归口。

本文件起草单位：。

本文件主要起草人：×××

零信任架构下的动态访问控制算法实施指南

1 范围

本文件规定了零信任架构下的动态访问控制算法的总则、总体架构、算法输入因子规范、算法类型及实施技术要求、全流程实施规范、访问决策与会话管控、隐私安全要求、测试验证、运维与审计等要求。

本文件适用于依据 GB/T 43696 建设的零信任安全系统，可用于零信任产品研发、安全方案设计、工程实施、安全测评、运维管理等相关工作。

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 22239 信息安全技术 网络安全等级保护基本要求

GB/T 25069 信息安全技术 术语

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 38664（所有系列） 信息技术 大数据 政务数据开放共享

GB/T 43696 网络安全技术 零信任参考体系架构

3 术语和定义

GB/T 25069、GB/T 43696 和 GB/T 38664（所有系列）界定的以及下列术语和定义适用于本文件。

3.1

零信任架构 zero trust architecture；ZTA

以“永不信任、始终验证”为核心，不基于网络位置预设信任关系，依托多维上下文持续评估实现动态授权的安全架构体系。

3.2

动态访问控制算法 dynamic access control algorithm

部署于零信任策略决策点（PDP），融合主体、设备、网络、行为、威胁、业务多维上下文特征，完成信任量化、风险判定、访问决策的标准化计算逻辑集合。

3.3

策略决策点 policy decision point；PDP

负责接收访问请求、执行访问控制判定、输出授权决策结果的逻辑功能组件。

3.4

上下文感知 context awareness

零信任架构中，实时采集、同步更新访问全维度环境与状态数据，为动态算法决策提供输入支撑的能力。

4 总则

4.1 实施原则

零信任动态访问控制算法实施，应严格遵循以下原则：

a) 最小权限原则：算法输出的访问权限范围，应不大于主体完成对应业务所需的最低权限；
b) 持续验证原则：访问授权不应为静态固化权限，应在会话周期内持续重评估；
c) 动态驱动原则：算法决策应以实时多维上下文为核心依据，不得仅依赖静态身份与网络位置；
d) 可审计可解释原则：所有算法决策过程、输入因子、判定依据应可追溯、可复盘、可解释；
e) 隐私最小化原则：数据采集与处理应符合 GB/T 35273 要求，仅采集算法必需数据；
f) 安全可用平衡原则：算法阈值与参数配置宜兼顾安全防护有效性与业务连续性。

4.2 算法架构定位

动态访问控制算法是零信任 PDP 的核心计算内核，承接多源上下文感知数据，输出标准化决策指令至 PEP，与身份治理、终端安全、威胁情报、行为分析系统联动协同。算法为授权决策核心逻辑，不替代身份认证、传输加密、终端防护等基础安全能力。

4.3 实施条件

开展动态访问控制算法落地实施前，应完成以下基础建设：

a) 依据 GB/T 43696 完成零信任基础架构部署；
b) 完成主体身份统一治理、资产资源分级分类；
c) 完成 PEP 网关、代理组件的链路部署；
d) 建立多源上下文数据采集与同步通道；
e) 建立符合等级保护要求的审计日志存储体系。

5 总体架构

动态访问控制算法实施体系自上而下分为五层架构，分别为上下文感知采集层、特征预处理层、信任评估决策层、决策指令执行层、反馈闭环迭代层。各层级解耦设计、标准化对接，支撑全流程动态访问管控：

a) 上下文感知采集层：本层级应汇聚身份、终端、网络、资源、行为、威胁、业务七大类数据，支持主动轮询、事件推送两种采集模式。所有采集数据应携带标准时间戳与唯一会话标识，保障时序一致性与可溯源性；
b) 特征与处理层：原始采集数据应经过标准化预处理后方可输入算法引擎，预处理包含数据清洗、重复剔除、缺失值补全、异常值过滤、特征归一化、离散特征编码、上下文快照固化。所有预处理规则应可配置、可审计、可追溯；
c) 信任评估决策层：算法引擎应支持规则驱动、加权评分、机器学习、混合架构四类算法形态，内置冲突裁决、阈值判定、分级决策能力。多算法并行输出不一致时，应执行预设优先级策略，保障决策唯一性；
d) 决策指令执行层：算法输出决策结果应包含请求唯一标识、主体标识、资源标识、决策动作、有效时长、约束条件、决策依据、置信度参数，支持 REST API、gRPC、OPA 标准协议对接 PEP 组件；
e) 反馈闭环迭代层：系统应持续采集决策执行结果、安全告警、人工复核记录、风险事件数据，形成标准化迭代数据集，支撑算法参数调优、规则更新、模型迭代。

6 算法输入因子规范

动态访问控制算法输入因子分为七大类，敏感核心资源访问场景应全覆盖主体、设备、网络、资源、威胁五类核心因子。

6.1 主体身份

包含主体唯一标识、认证方式、认证强度、角色权限基线、特权账号标识、主体信用基线等参数，用于判定主体身份可信等级。

6.2 设备状态

包含设备唯一指纹、设备归属类型、系统补丁状态、安全软件运行状态、设备合规得分、越狱/ROOT状态、恶意进程检测状态等参数。

6.3 网络环境

包含接入 IP、接入网络类型、传输加密状态、IP 信誉等级、代理/VPN 使用状态、接入地理位置粗粒度信息等参数。

6.4 访问资源

包含资源敏感等级、资源安全基线、访问黑白名单、资源运行风险状态等参数。

6.5 用户行为

包含访问时段、访问频次、历史访问基线、操作行为序列、异常行为标记、会话持续时长等参数。

6.6 威胁情报

包含 IP 威胁标签、设备风险标记、主体异常行为告警、全局安全预警等级等参数。

6.7 业务合规

包含业务允许访问时段、审批流程状态、数据合规访问约束、行业监管限制条件等参数。

7 算法类型及实施技术要求

7.1 规则驱动型算法

基于预设条件规则集完成布尔逻辑判定，适用于合规要求明确、场景固定的政企场景。规则应版本化管理、支持冲突检测、优先级排序，所有规则变更应留存审计记录。

7.2 加权评分型算法

对多维因子配置合规权重与分值，实时计算综合信任得分，通过阈值比对输出分级决策。权重配置应基于风险评估确定，支持按资源等级差异化配置，评分明细应全程可追溯。

7.3 机器学习型算法

基于合规脱敏数据集训练模型，识别未知异常访问风险。模型训练与迭代应符合个人信息保护要求，系统应配置模型漂移监控、灰度验证、人工复核机制。

7.4 混合架构算法

采用“规则基线+模型增强”的主流落地架构，规则算法保障基础安全与可解释性，机器学习模型提升未知风险识别能力。系统应配置降级机制，模型异常时自动切换至规则/评分算法。

8 全流程实施规范

动态访问控制算法实施应依次完成需求梳理、通道建设、算法设计、系统集成、灰度调优、正式上线、持续迭代六个阶段，禁止直接全量上线。

8.1 需求梳理与资产建模

本阶段为算法实施基础阶段，应结合业务场景、安全合规要求、资产风险等级完成全维度梳理与建模，输出可落地的实施基线。具体工作内容如下：

a) 资产梳理与分级分类：依据 GB/T 22239 安全防护等级要求，对业务系统、数据库、API 接口、文件资源、服务负载、物联网设备等访问客体进行分级，划分为一般、重要、核心三级资产，明确不同等级资产的访问安全基线与风险管控阈值；
b) 主体梳理：全覆盖梳理自然人用户、运维账号、业务服务账号、终端设备、第三方接入主体，明确特权账号、普通账号、匿名访问主体的差异化管控要求，完成主体唯一身份标识统一归集；
c) 业务场景梳理：梳理南北向远程办公访问、内网终端业务访问、数据中心东西向服务互访、工业设备联网访问、第三方外协接入等全场景访问链路，明确各场景的业务特性、访问时段、权限诉求与可接受风险等级；
d) 算法选型定位：结合资产等级与场景复杂度选定适配算法类型，低风险固定合规场景选用规则驱动算法，中等风险混合办公场景选用加权评分算法，高风险核心资产、未知威胁防护场景选用机器学习或混合架构算法；
e) 输出成果：形成《零信任动态访问控制算法需求规格说明书》《资产分级分类清单》《主体访问场景台账》，作为后续算法设计、部署、调优的唯一依据。

8.2 数据采集通道建设

本阶段核心是搭建稳定、实时、合规的多源上下文数据采集通道，保障算法输入数据的完整性、时效性、准确性，具体实施要求如下：

a) 数据源对接适配：对接统一身份管理平台、终端安全管理系统、网络设备、威胁情报平台、UEBA 用户行为分析系统、业务管理系统，覆盖本文件 6 章节规定的七大类输入因子；支持主动轮询、事件主动推送两种采集模式，高频风险因子采用事件推送模式，基础稳态因子采用定时轮询模式；
b) 通道技术规范：数据传输应采用 TLS1.3 及以上加密协议，禁止明文传输上下文敏感数据；支持 REST API、gRPC、消息队列等主流对接方式，适配国产化软硬件环境；所有数据交互应携带唯一会话 ID 与标准时间戳，保障数据时序一致性与链路可溯源；
c) 数据质量管控：设置数据采集心跳检测机制，实时监测各数据源在线状态，对离线、超时、异常数据进行标记隔离；配置数据重复剔除、时序错乱修复机制，规避脏数据导致的算法决策异常；
d) 合规适配：严格遵循 GB/T 35273 个人信息最小化采集原则，仅采集算法决策必需的特征数据，禁止无差别采集用户隐私、精准位置、生物特征等非必要信息；
e) 通道验收：完成通道搭建后，应开展 72 h 稳定性测试，验证数据采集成功率、延迟、完整性满足业务要求，形成数据采集通道验收报告。

8.3 算法规则与参数配置

基于前期需求梳理成果，完成算法规则编写、权重配置、模型训练、阈值设定，构建完整可运行的算法决策体系，具体实施要求如下：

a) 规则体系搭建（规则/混合算法适用）：依据合规要求、资产等级、风险基线编写标准化访问控制规则，涵盖身份合规、设备合规、网络合规、行为合规、威胁规避五大类规则；设置规则优先级机制，核心资产防护规则优先级高于通用业务规则，同时配置规则冲突检测与自动告警机制；所有规则实行版本化管理，留存变更日志；

b) 权重参数配置（评分/混合算法适用）：基于风险评估结果为七大类上下文因子分配差异化权重，核心风险因子（设备合规、威胁情报、身份认证强度）配置高权重，稳态业务因子配置常规权重；支持按资产等级、访问场景配置多套权重模板，禁止全局统一权重配置；所有权重参数变更需经安全管理员审批；

c) 模型训练调优（机器学习/混合算法适用）：采用脱敏后的合法历史访问数据集开展模型训练，剔除违规数据、隐私数据；选用逻辑回归、随机森林、梯度提升等适配零信任场景的轻量模型，兼顾识别精度与推理时延；完成模型训练后开展离线仿真测试，验证模型对异常访问、风险行为的识别能力；

d) 阈值体系设定：结合业务容忍度与安全防护要求，设定高可信、中风险、高风险三级信任阈值，匹配差异化管控策略；区分工作时段、非工作时段、节假日配置差异化阈值，适配真实业务运行规律；

e) 离线验证：完成参数与规则配置后，开展全场景离线仿真，覆盖正常访问、异常访问、数据缺失、设备异常、异地登录等典型场景，确保算法决策逻辑合规、有效。

8.4 PDP/PEP 系统集成联调

完成算法引擎与零信任控制中心、PDP、PEP 组件的全链路集成联调，打通数据流转、决策输出、指令执行全流程，具体实施要求如下：

a) 引擎集成：将调试完成的算法引擎部署至零信任 PDP 核心模块，实现上下文数据自动接入、算法自动调度、决策自动输出；配置引擎异常降级机制，算法服务故障时自动切换至兜底安全策略，保障业务不中断、安全不失效；

b) 接口联调：依据标准化协议完成 PDP 与 PEP 接口对接，确保决策指令可实时、准确下发至网关、代理、终端准入等 PEP 组件；联调验证决策字段完整性，包含请求 ID、主体标识、资源标识、决策动作、有效时长、决策依据等必填字段；

c) 全链路测试：模拟全场景访问请求，验证“数据采集-特征预处理-算法决策-指令执行-日志留存”全链路闭环；重点测试多算法并行场景下的冲突裁决逻辑、权限动态更新逻辑、会话重评估触发逻辑；

d) 权限与安全加固：对算法引擎、参数配置、规则库、模型文件设置最小权限管控，禁止越权查看、修改、删除核心配置；加固接口访问权限，防止非法调用、伪造请求欺骗算法引擎；

e) 联调验收：排查全链路异常问题，修复时延过高、决策失效、指令不执行等问题，形成系统集成联调报告，具备灰度试运行条件。

8.5 灰度试运行与阈值调优

为规避全量上线导致的业务中断、误阻断、安全漏防风险，必须开展分阶段灰度试运行，完成算法参数、阈值、规则的精细化调优，具体实施要求如下：

a) 灰度范围划分：遵循“从低风险到高风险、从非核心业务到核心业务”的灰度原则，优先对普通办公、非核心业务系统开放算法管控，逐步拓展至重要、核心资产场景；禁止核心业务、关键数据系统直接全量上线；
b) 试运行观测：灰度周期不少于 7 个自然日，全程监控算法决策分布、访问阻断率、误判率、业务故障率、算法响应时延等核心指标；统计正常访问误阻断、异常访问漏放行、风险场景未识别等问题台账；
c) 精细化调优：基于试运行数据，优化因子权重、信任阈值、规则优先级；针对高频误判场景优化特征预处理规则，针对漏防风险场景补充风险识别规则、调高高危因子权重；区分不同时段、不同接入环境差异化优化参数；
d) 人机协同校验：灰度期间开启人工复核机制，对中风险、高风险决策结果进行人工二次校验，比对算法决策与人工判定差异，迭代优化算法模型与规则体系；
e) 灰度验收：试运行期间无重大业务故障、无高危安全漏防、误阻断率符合业务容忍标准后，出具灰度试运行报告，准予全量上线。

8.6 正式上线与常态化迭代

完成灰度验收后全量启用动态访问控制算法，建立常态化运维、复盘、迭代机制，持续适配业务变化与新型安全风险，具体实施要求如下：

a) 全量上线部署：分批次完成全业务、全资产、全主体的算法管控覆盖，关闭临时兜底调试策略，启用正式算法决策体系；上线后 24 h 全程值守监控，及时处置突发异常；
b) 常态化运行监控：按照本文件第 12 章要求，实时监控算法吞吐量、响应时延、决策准确率、数据源稳定性、异常告警数量等指标，建立日监控、周汇总、月复盘机制；
c) 周期性迭代优化：每季度开展一次算法全面复盘，结合业务变更、资产新增、安全事件、威胁情报更新情况，优化规则库、权重参数、模型版本；针对新增业务场景、新型网络攻击手段，及时补充风险识别规则；
d) 版本迭代管理：算法规则、参数、模型迭代实行版本化管控，留存迭代记录、测试报告、审批记录，确保迭代过程可追溯、可回滚；重大迭代需再次开展灰度测试，验证无误后全量更新；
e) 场景适配更新：当企业 IT 架构、接入场景、合规要求发生变更时，即时启动算法适配优化，保障动态访问控制能力持续匹配业务与安全需求。

9 访问决策与会话管控

9.1 基础决策动作

算法决策应至少支持允许访问、受限访问、二次认证、拒绝访问四类标准动作。

9.2 分级动态管控

依据信任得分划分高可信、中风险、高风险三级管控区间，匹配差异化安全策略。

9.3 会话持续重评估

系统应支持周期重评估与事件触发重评估，会话权限动态更新，禁止长期静态授权。

9.4 权限升降级机制

信任状态恶化时自动降级权限，风险消除后应重新完成评估方可恢复权限。

10 隐私安全要求

所有数据采集、传输、存储、使用应符合 GB/T 35273 规范。算法参数、规则模型应做权限管控与防篡改保护。所有决策行为应满足等级保护审计要求。

11 测试验证

11.1 功能测试

功能测试应验证算法决策逻辑、流程链路、输出结果符合本文件规范及预设安全策略，测试覆盖要求如下：

a) 常规场景测试：测试正常身份、合规设备、安全网络环境下的业务访问，验证算法正常授权、会话持续评估功能正常；
b) 风险场景测试：模拟设备不合规、异地异常登录、高危 IP 接入、特权账号违规操作、高频异常访问等场景，验证算法可精准识别风险并执行限制、二次认证、阻断等管控动作；
c) 边界场景测试：测试信任阈值临界值、权重参数边界、数据极值等场景，验证算法决策逻辑无错乱、无失效；
d) 功能联动测试：验证算法决策与 PEP 执行、日志审计、告警推送、权限升降级功能联动正常，无链路断层。

11.2 性能测试

性能测试保障算法满足业务高并发、低时延运行要求，核心测试指标与要求如下：

a) 单请求评估时延：常规场景算法单次决策总时延应≤100 ms，核心低时延业务场景应≤50 ms，保障用户访问体验；
b) 并发处理能力：支持不低于业务峰值并发请求量的算法评估处理，无请求堆积、超时、丢失问题；
c) 资源占用率：算法引擎运行期间服务器 CPU、内存占用率应控制在业务容忍范围内，长期运行无内存泄漏、性能衰减问题；
d) 持续运行稳定性：开展 72 h 压测，验证高并发场景下算法决策准确率、时延指标无异常波动。

11.3 安全有效性测试

安全有效性测试用于验证算法风险防护能力，抵御各类非法访问与攻击行为，测试内容如下：

a) 凭证风险测试：模拟账号密码泄露、令牌被盗用、静态凭据复用等场景，验证算法可通过多维上下文差异识别非法访问；
b) 终端失陷测试：模拟终端植入恶意程序、设备越狱/ROOT、安全软件失效等场景，验证算法及时判定高风险并阻断访问；
c) 网络攻击测试：模拟代理伪装、VPN 异常接入、恶意 IP 扫描、跨境非法访问等场景，验证算法联动威胁情报实现风险拦截；
d) 权限滥用测试：模拟越权访问、批量访问核心资源、非工作时段违规操作等行为，验证算法可动态降级权限、阻断异常操作。

11.4 鲁棒性测试

鲁棒性测试验证算法在异常工况下的容错能力与安全兜底能力，具体要求如下：

a) 数据异常测试：模拟数据源离线、特征数据缺失、数据篡改、脏数据接入等场景，验证算法不崩溃、不失效，可触发降级安全决策；
b) 服务异常测试：模拟算法引擎瞬时故障、接口超时、服务重启等场景，验证系统自动切换兜底策略，保障安全可控；
c) 极端并发测试：模拟瞬时超高并发、突发批量访问请求，验证算法无决策错乱、无安全旁路；
d) 测试结论要求：所有异常场景均需形成测试记录，针对容错短板优化算法参数与兜底策略。

12 运维与审计

12.1 运维监控

系统应搭建可视化监控体系，常态化监测算法运行核心指标，包含：
a) 运行状态指标：算法引擎在线状态、数据源接入成功率、接口调用成功率、服务可用性；
b) 性能指标：单次决策平均时延、最大时延、并发处理吞吐量、资源占用率；
c) 决策统计指标：允许、受限、二次认证、拒绝四类决策占比，误判、漏判事件数量；
d) 风险告警指标：高风险访问次数、异常行为触发次数、设备/网络风险告警数量；
e) 监控预警机制：为核心指标设置阈值告警，指标超标时及时推送告警信息，实现早发现、早处置。

12.2 审计日志要求

12.2.1 严格依据 GB/T 22239 等级保护日志留存要求，搭建不可篡改审计日志体系，日志应包含以下核心字段：
a) 时间戳；
b) 唯一会话 ID；
c) 主体唯一标识；
d) 设备指纹；
e) 网络环境信息；
f) 访问资源信息；
g) 全量输入因子快照；
h) 算法类型；
i) 决策依据、决策结果；
j) 执行动作；
k) 操作人员；
l) 参数变更记录等。

12.2.2 日志留存周期不应少于 6 个月，核心涉密场景留存周期不少于 1 年，支持日志检索、溯源、报表导出。

12.3 应急处置

为应对算法故障、异常决策、业务中断等突发情况，应建立专项应急处置机制：
a) 应急预案制定：预设算法服务宕机、大规模误阻断、高危漏防、数据异常等场景应急预案，明确处置流程、责任人、恢复时限；
b) 临时兜底策略：配置安全优先、业务优先两类可一键切换的兜底策略，仅用于应急故障处置，禁止长期使用；兜底策略开启后需全程记录、事后复盘；

c) 故障排查机制：建立快速排查链路，针对算法逻辑、数据源、接口、部署环境等维度分层排查故障原因；

d) 事后复盘整改：应急处置完成后，24 h 内完成事件复盘，优化算法短板与运维机制，杜绝同类故障重复发生。