2025年浙江省信息通信业职业技能竞赛

数据安全管理员

竞赛技术文件

**2025年7月**

目录

[一、 竞赛概述 3](#_Toc47674656)

[二、 竞赛内容 3](#_Toc1022110535)

[2.1初赛赛段 4](#_Toc1879503977)

[2.2决赛赛段 4](#_Toc470477179)

[三、 竞赛规则 4](#_Toc1802351408)

[3.1初赛赛段 4](#_Toc1630069746)

[3.2决赛赛段 5](#_Toc1355179278)

[3.3评判方法 5](#_Toc608851388)

[3.4申诉与仲裁 6](#_Toc847339528)

[四、 竞赛场地与设备 6](#_Toc1011939793)

[4.1赛项设备配备情况 6](#_Toc1428456731)

[4.2、竞赛平台页面（样式参考，以大赛实际平台为准） 8](#_Toc752526620)

[4.3、竞赛场地要求 9](#_Toc1783947538)

[五、 注意事项 10](#_Toc552460257)

[5.1初赛注意事项 10](#_Toc2113611113)

[5.2决赛注意事项 10](#_Toc562685200)

[附件一：赛题大纲 12](#_Toc394077044)

[附件二：参赛选手工具清单 15](#_Toc1930933096)

# 竞赛概述

为深入贯彻落实党的二十大报告关于强化网络、数据等安全保障体系建设的重大决策部署，紧密结合浙江在数字经济领域的领先地位与蓬勃发展态势，积极响应全国电信和互联网行业关于推动行业人才交流的号召，秉持“以赛促学、以赛促练”的宗旨，开展实战、场景竞赛，促进行业数据安全高技能人才队伍发展，助力支撑加快推进浙江省新型工业化和网络强省建设。

竞赛以《国家职业技能标准》中关于数据安全管理员高级工（国家职业资格三级）的要求为基础，适当增加技师（国家职业资格二级）内容及相关新知识、新技能，从政策法规标准、网络安全、数据安全等技术要点展开，全方位考核参赛选手的网络安全和数据安全综合能力。

# 竞赛内容

竞赛围绕算力网络、5G网络、人工智能、软件供应链等重点业务和应用方向，针对数据窃取、数据加密、恶意流量攻击等纷繁复杂安全事件的检测、防御和处置工作内容，结合联防联控、实战指挥体系下的岗位设置及人员技能需求，面向电信和互联网重要业务场景下典型、高水平安全风险的防范应对，以理论考察、实践操作等多种形式，充分考察参赛选手各项安全技能掌握水平。

竞赛分为初赛和决赛两个赛段。

## 2.1初赛赛段

初赛通过线上选拔方式，采用个人赛"理论考核+实战解题"模式。理论考试侧重网络安全政策法规、标准规范等基础知识测评；实战解题环节聚焦数据安全、系统安全、移动安全、云安全、密码学等核心领域。

## 2.2决赛赛段

决赛采用线下方式，分为个人赛和团队赛两个环节，个人赛采用"理论考核+实战解题"模式，团队赛环节采用综合场景题模式。

理论考核部分涵盖数据安全、系统安全、网络安全、软件安全、移动安全、安全法规及相关标准等知识点；实战解题部分聚焦网络安全和数据安全核心领域，设置数据安全管理、加密流量分析及追踪、综合情报分析、应急响应、数字取证、综合渗透等实操题型。

团队赛环节采用综合场景题模式，赛题聚焦数据安全全生命周期及常规网络安全应急处置，场景设计涵盖敏感信息泄露防护、数据分类分级管理、细粒度权限控制等实际业务痛点，并融入数字水印技术、常见加解密算法等关键技术应用，全面评估团队的技术实力和协作能力。

# 竞赛规则

## 3.1初赛赛段

初赛比赛时长240分钟，前60分钟进行理论考试，后180分钟进行实战解题，比赛开始时同步放出理论答题界面和实操界面，比赛开始60分钟后关闭理论答题界面。

初赛总分为1000分，其中理论考核200分，实操考核800分。

## 3.2决赛赛段

决赛个人赛比赛时长180分钟，前60分钟进行理论考试，后120分钟进行实战解题，比赛开始时同步放出理论答题界面和实操界面，比赛开始60分钟后关闭理论答题界面。

决赛团队赛比赛时长180分钟，主要是数据安全场景实操考核。

决赛个人赛和团队赛总分均为1000分，其中个人赛理论考试200分，夺旗实操考核800分；团队赛场景考核总分1000分。参赛选手需在规定时间内作答，提交正确答案得分，并按分数高低决出本次比赛的优胜者。如出现同分现象，先达到实操考核成绩最终分数者排名靠前。

## 3.3评判方法

1. 理论考试中参赛选手需根据题目描述，选择合适选项进行作答，题目作答过程中计时不中断，参赛选手作答完毕点击交卷完成理论考试，若在规定时间内未完成交卷，系统自动提交计分。
2. 数据安全实战解题和数据安全场景实操考核每道题目有且仅有一个正确Flag，参赛选手根据题目要求格式提交，通过提交Flag验证，系统自动计分。

## 3.4申诉与仲裁

在竞赛过程中若出现有失公正、选手对成绩有异议、有关人员违规等现象，各领队可在比赛结束后1小时之内向大赛组委会办公室提出书面申诉，非书面申诉不予受理。书面申诉应对申诉事件的现象发生时间、涉及人员等行实事求是的叙述，并提供事实依据(无事实依据或主观臆断不予受理)，经各领队亲笔签名后提交。大赛组委会办公室在接到书面申诉后2小时内组织相关人员复议，并及时将复议结果以书面形式告知申诉方。

# 竞赛场地与设备

## 4.1赛项设备配备情况

**（1）赛项平台技术参数**

主要参数规格如下：

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 型号规格 |
| 1 | 硬件及性能 | 型号戴尔R7525 2U机架式服务器 |
| 处理器：AMD EPYC 7H12\*2 单颗64核心128线程，主频2.6GHz |
| 内存：64G DDR4 3200MHz\*8 |
| 硬盘储存：1.92T\*3 |
| 整列卡：H745 |
| 网络：双口千兆，双口万兆(含模块) |
| 电源：1300W\*2 |
| 并发虚拟机数量≥100 |
| 2 | 竞赛平台功能模块 | 1. 多赛事并发与配置能力  本竞赛平台支持多场赛事的并发运行，具备资源隔离与独立调度能力。赛事基本信息可灵活配置，包括名称、时间、组别、赛制模式等关键参数，满足不同组织单位的办赛需求。平台支持理论考试、CTF、CFS、AWD、RDG、应急响应、安全运维等多种赛制，允许灵活组合，并可设置固定计分、动态计分、首血/次血加成等多样化计分机制，实现多维度考评目标。  2. 展示界面与环境配置能力  平台提供前台展示信息的自定义功能，支持设置名称字号、示例图、用户昵称保护策略、排行榜样式、背景风格、赛事公告等。系统集成作弊监控机制，可对参赛选手的动态Flag使用行为、IP绑定记录、可疑操作行为等进行分析，辅以处罚机制，确保赛事公平。题目环境的启动时长、自动释放时间均可灵活配置，管理员具备环境延时、重启、释放等操作权限，保障比赛流畅运行。  3. 赛事人员管理功能  支持对参赛人员和观摩人员的独立管理，个人赛按用户单元管理，团队赛以队伍形式批量管理。管理员可进行人员添加、审核、批量移除、批量审核、一键导出等操作，同时支持从系统人员库中快速导入参赛人员。  4. 赛段配置机制  系统支持多赛段并发运行，并可对每个赛段单独配置时间与模式。理论考试支持固定时长与固定时间两种方式，题目顺序支持顺序与乱序出题。CTF赛段支持固定计分、动态计分、首血奖励等机制，AWD模式则可设置加固阶段及环境重置策略，以适配攻防对抗不同阶段的需求。  5. 题目管理系统  平台支持题目的编辑、删除、导入、导出、上下线、分值调整、出题顺序设定等操作。支持多种题型，包括单选、多选、判断、填空、CTF、CFS、AI安全等题型，Flag形式支持静态、动态等方式，题目结构可为环境类、外链类、附件类。  6. 环境与资源管理  竞赛平台支持基础计算环境、KVM虚拟环境以及AI模型数据安全仿真环境的统一管理。平台具备图形化拓扑结构展示能力，选手可通过拓扑图直接进入靶机环境进行操作。管理员可实时查看选手环境运行状态，支持对环境进行手动延时、强制重启与释放操作，提升赛事环境的动态管理能力。  7. 赛事公告与动态发布  平台支持管理员在比赛过程中实时发布公告信息，包括比赛通知、题目变更、违规警告、新消息提示等内容。赛事动态可实时记录参赛人员答题进度、操作行为与成绩情况，支持动态信息的导出与历史记录管理，用于赛后分析与复盘。  8. 日志记录与异常行为分析  系统自动记录赛事过程中的日志数据，包括理论考试日志、CTF答题记录、AWD对抗日志、CFS操作日志等。异常分析模块支持对作弊行为进行监控和分析，记录动态Flag使用、IP绑定变化、登录行为等，可生成处罚信息、支持导出与清空相关记录，并将结果反馈至平台管理端。  9. Writeup 提交与综合排行  平台支持选手在比赛过程中提交 Writeup（解题过程与思路），管理员可对提交内容进行文件查看、审核或统一清空。系统统计所有赛段分数与排名数据，支持导出排行榜。平台支持个人的排名展示，并具备大屏可视化观摩功能，实时展示赛事战况、选手头像、答题进度等内容。 |

## 4.2、竞赛平台页面（样式参考，以大赛实际平台为准）



图 1：竞赛平台登录页面



图 2：数据安全夺旗赛答题页面

图 3：数据安全综合场景赛答题页面

## 4.3、竞赛场地要求

（一）面积不小于400平方米的场地，分为竞赛场地、大屏展示、数据中心、裁判室、储物间、观摩等区域。

（二）竞赛区域搭建有线局域网，个人赛设置150个工位（含备用工位），工位间距不低于1.8米，每个工位桌接入电源和网线；现场电源功率不低于30kW，尽量双路电源，且配备UPS。

（三）2台信号屏蔽器，能够屏蔽竞赛现场4G、5G等信号源。

（四）2台高性能硬件服务器，2台算力服务器，1台赛事展示大屏电脑，1个成绩展示大屏。

（五）竞赛场地照明应充足、柔和，赛场需留有安全通道，并设置显著标识;配备灭火设备，备有通风设备，保证空气流通和清洁。

# 注意事项

## 5.1初赛注意事项

1. 严禁任何作弊行为，一经发现立即取消参赛资格。
2. 在比赛过程中，参赛选手严禁向比赛服务器、其他参赛选手个人电脑等设备发起任何可能影响比赛的攻击行为，一经发现立即取消参赛资格。
3. 比赛结束后4小时内，各参赛队伍需在竞赛平台完成writeup提交，过期视为放弃比赛成绩。

## 5.2决赛注意事项

1. 参赛选手凭本人身份证签到后进入赛场，对号入座，不得擅自更换座位。
2. 参赛选手须提前30分钟入场，测试网络连通性及竞赛系统账号和口令，迟到超过30分钟禁止入场，并按弃权处理，已检录入场的参赛选手未经允许，不得擅自离开赛场。
3. 比赛时，参赛选手严禁携带手机等与比赛无关的具有通信功能电子设备（包括但不限于智能手表、手环、蓝牙耳机、智能眼镜等）等物品进入赛场，禁止携带网络安全类硬件设备进入赛场等互联网通讯设备带入比赛场地。
4. 参赛选手须自带稳定可用的笔记本电脑参加竞赛，并自行配置有线网口和有线鼠标，自行准备工具和软件。若出现因自带电脑原因无法连接竞赛系统的情况，责任自负。
5. 比赛过程中，参赛选手严禁向比赛服务器、其他参赛选手个人电脑等设备发起任何可能影响比赛的攻击行为。
6. 比赛过程中，场地内将开启信号屏蔽器等设备，屏蔽现场的手机信号和WLAN等。
7. 比赛过程中，参赛选手若遇技术故障，应举手询问现场监考人员。
8. 比赛过程中，参赛选手请遵守工作人员指示，尊重裁判裁决。
9. 当裁判宣布比赛结束时，所有参赛选手应立即停止所有操作。

一经发现参赛选手出现违反竞赛纪律的行为，组委会视情节轻重给予警告、扣分公开警告、终止比赛资格并通报所在单位、列入本大赛黑名单等处罚。

# 附件一：赛题大纲

法律法规：了解相关网络安全防护范围、管理主体、责任主体、同步要求、分级备案要求、符合性评测要求、风险评估要求、应急演练要求等内容。

政策文件：了解电信网络安全防护工作总体思路、基本原则、主要任务、实施及监督检查要求、安全服务机构管理等政策文件；了解电信网络等级保护工作的目的、原则、意义、要求、思路、实施内容、流程等政策内容；熟悉电信网络等级保护定级范围、评审要求、备案等政策要求，熟知电信网络单元安全防护定级方法、定级对象命名规则、定级报告内容、定级备案相关信息等。深入了解运营商行业信息安全管理体系认证相关工作的目的、意义以及要求。

网络安全防护相关标准：了解安全防护定义、目标、基本原则、体系及各部分工作内容等内容。熟悉安全等级划分、定级对象划分、定级方法及要素、等级保护原则和实施过程等相关标准；了解安全风险评估要素及关系、工作形式、遵循原则、实施流程、在不同生命周期中的要求和实施要点等标准；了解灾难备份等级划分、灾难备份原则、灾难备份资源要素、实施过程、灾难恢复预案要求等防护标准。

数据安全：熟练使用加密技术进行数据加密，掌握数据脱敏能力，精准的数据访问权限控制能力，了解数据泄漏保护策略，了解分布式存储技术。熟练掌握数据备份与恢复技术。

操作系统安全检测与防护：了解操作系统（Windows、Linux、Unix 等）的常规安全防护技术；能熟练利用系统日志、应用程序日志等溯源攻击途径；掌握系统账号、文件系统、网络参数、服务、日志审计等项目的安全检测与安全加固方法。

数据库安全检测与防护：了解数据库（Mssql、Mysql、Oracle、MongoDB）的库表管理、权限控制等数据库管理方式；熟悉数据库入侵防御、访问身份认证、数据加密等其他安全措施；深入了解数据库的客户端程序管理、应用系统访问、客户端访问控制、重要操作审计以及数据备份。

网络攻击与防护：熟悉网络层攻击原理及防护方法，能运用相关工具及技术手段发现并阻断网络层攻击、验证无线网络 WEP、WPA 和 WPA2 的密码强度。

Web 应用安全：了解常见 Web 环境（ASPX、PHP、JSP）的搭建方法以及安全配置方法；熟悉中间件和 Web 应用的安全检测与防护方法。

渗透测试技术：掌握常规的渗透测试技术；熟悉使用各种常见渗透测试工具。

应急响应与数据恢复：掌握应急响应和数据恢复的流程和相关技术，包括：入侵取证分析、反取证技术、日志审计分析、日志删除恢复、文件删除恢复、硬盘格式化数据恢复等。

开发安全：了解常见编程环境（C、JAVA、PHP、JSP）的构建以及语言的编写；熟悉缓冲区溢出、拒绝服务等编码防御技术；掌握代码审计和代码加固技术，避免出现常见安全漏洞。

恶意代码与逆向：熟悉操作系统中恶意代码的识别方法及防护措施，能运用相关工具及技术手段发现、隔离、清除常见恶意代码。

移动应用安全：了解移动智能终端操作系统、移动应用软件的常规安全漏洞检测和防护技术；熟悉移动互联网恶意程序相关监测与处置机制；掌握移动应用的逆向分析和代码审计技术、移动应用的安全防护方法等。

新技术应用：了解云计算与大数据的基本概念及特征；熟悉云计算和大数据技术带来的安全问题；掌握如何使用大数据分析安全事件以及大数据平台本身安全漏洞和隐患的发现。

# 附件二：参赛选手工具清单

选手自带工具清单表如下：

| 序号 | 名称 | 数量 | 说明 |
| --- | --- | --- | --- |
| 1 | 笔记本电脑 | 1台 | Intel Core i7 或 AMD Ryzen 7 处理器，32GB DDR4 内存，1TB NVMe SSD，NVIDIA GeForce RTX 3060显卡，操作系统（Windows 10/11、 Kali Linux等），以太网接口，无线网络适配器。 |
| 2 | 有线鼠标 | 1个 | 有信号屏蔽仪，请尽量带有线鼠标键盘。 |
| 3 | RJ45接口转换器 | 1个 | 若笔记本电脑无网口，需自备。 |