《电力企业网络安全蜜罐部署与管理技术规范》

编制说明（征求意见稿）

一、工作简况

1 主要工作过程

起草（草案、调研）阶段：

2024 年 1 月，成立标准起草工作组，确定主笔人、起草单位，确定工作方法及工作内容，开展课题前期研究工作。2024 年 2 月至 5 月，启动团体标准编制工作，形成《电力企业网络安全蜜罐部署与管理技术规范》立项申请书与草案，并提交至中国电工技术学会。2024 年 5 月邀请相关专家对草案进行讨论与研究，标准起草工作组根据专家意见对草案进行补充与完善，形成标准征求意见稿。

2 主要参加单位和起草工作组成员及其所做的工作

标准编写组收集了近几年来企业网络安全蜜罐部署与管理方面的相关资料，通过对比整理分析确定了标准主要技术内容，由国网山西省电力公司电力科学研究院、国网信息通信产业集团有限公司牵头完成标准编制、整理和完善，其他参与单位配合并负责收集相关资料、提出建议。

主要参与单位：国网山西省电力公司电力科学研究院、国网信息通信产业集团有限公司、四川中电启明星有限公司、华北电力大学、安徽继远检验检测技术有限公司、北京中电普华信息技术有限公司，南京南瑞信息通信科技有限公司。

主要参与人员：刘泽辉、付昀夕、芦山、张敏、杨华、马东娟、周自强、刘泽三、宫晓辉、凌浩洁、高紫婷、闫廷廷、王振亚、张文娟、闫晨阳、黄元、李杉、李廷顺、靳鑫、杨姝、任彦斌、宋亚琼、王军、潘安顺、富思、沈耀威、韩泽华、苑学贺、董爱强、刘振圻、南淑君。

二、标准编制原则和主要内容

1、标准编制原则

a.本标准的起草遵循《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，以科学性、先进性和经济性为原则，坚持实事求

是，遵守国家有关法律、法规，同时符合团体标准要求。本标准旨在为企业网络安全领域提供一个关于蜜罐部署与管理的综合性框架，包括但不限于基本架构、部署策略和管理流程的具体要求。通过实施这些标准，企业能够更有效地保护其网络资产和信息安全，确保业务流程的连续性和稳定性。

b.采用会议讨论的形式，集合信息技术、电力技术、网络安全等专家，将不同业务维度的专业技术融合一体，体现出标准编制的科学性、实用性和先进性。

2、标准主要内容

本标准分为 7 个章节，（1）范围；（2）规范性引用文件；（3）术语和定义；（4）符号、代号和缩略语；（5）概述：介绍蜜罐分类、蜜罐变种以及蜜罐的应用场景；（6）企业网络蜜罐部署：介绍蜜罐部署位置、蜜罐部署功能选择、蜜罐部署配置、蜜罐部署攻击防范以及蜜罐部署合规性与隐私保护；（7）企业网络蜜罐管理：介绍蜜罐的维护更新、监控分析、响应处置与审查改进。

3、主要技术差异

本标准为新制度标准，无主要技术差异。

4、解决的主要问题

本标准主要解决的是未知威胁的监测与发现、攻击行为的实时分析与情报收集、降低真实系统的风险、提升安全团队的应急响应能力以及增强企业整体的安全防护能力等问题。

三、主要试验（或验证）情况

本标准不涉及试验（或研制）情况。

四、标准中涉及专利的情况

本标准不涉及专利问题。

五、预期达到的社会效益、对产业发展的作用等情况

1.提供丰富的蜜罐部署功能选择，包括但不限于数据捕获、实时监控、自动报警以及日志管理等。企业在实施蜜罐部署策略时，需根据自身的安全防护需求、网络架构特性以及可用资源情况，进行灵活的蜜罐类型选择、部署位置规划及功能配置，以实现最优化的安全防护效果。

2.充分考虑蜜罐部署的合规性与隐私保护，这涉及到明确界定法律合规框架、制定蜜罐数据管理的基本原则，以及构建跨部门协作整合的策略。通过这些措施，

可以确保蜜罐技术在网络安全防护中发挥其应有的作用，同时为企业的可持续发展提供坚实的保障。

3.定义企业业网络蜜罐管理的一系列关键活动和策略，包括蜜罐系统的定期维护与更新、持续的安全监控与行为分析、对可疑活动的快速响应与处置，以及对蜜罐策略的定期审查与改进。通过这些关键活动的系统化实施，可以不断提升蜜罐技术在企业网络安全防护中的实际效能。

六、与国际、国外对比情况

本文件未采用国际、国外标准。

七、在标准体系中的位置，与现行相关法律、法规、规章及相关标准，特别是强制性标准的协调性

本标准与现行的相关法律、法规、规章与相关标准保持一致。

八、重大分歧意见的处理经过和依据

标准编制过程中广泛征集了专家意见，所有意见均按照标准编制程序进行了采纳，不存在重大分歧意见。

九、标准性质的建议说明

建议本团体标准的性质为推荐性团体标准。

十、贯彻标准的要求和措施建议

建议本标准批准发布 7 天后实施。

十一、废止现行相关标准的建议

无

十二、其他应予说明的事项

无