ICS 35.030
CCS L 80

团　　体　　标　　准

T/ CIIPA 00012—2024

自主可控网络安全技术　基于网络靶场的软件自主可控能力测试指南

Autonomous and controllable cybersecurity technology—Guideline for testing the autonomous and controllable capabilities of software based on cyber range

2025-06-09 发布　　2025-06-11 实施

中关村华安关键信息基础设施安全保护联盟　发布
中　国　标　准　出　版　社　出版

目　　次

前言 ……Ⅲ
引言 ……Ⅳ
1　范围 ……1
2　规范性引用文件 ……1
3　术语和定义 ……1
4　缩略语 ……2
5　概述 ……3
5.1　软件自主可控能力测试范围……3
5.2　软件自主可控能力管理粒度……3
5.3　软件自主可控能力测试框架……3
5.4　软件自主可控能力评估……4
5.5　基于网络靶场的测试管理……4
6　软件资产自主可控能力测评方法 ……4
6.1　建立基础库……4
6.2　资产信息初始化……5
6.3　静态测试……5
6.4　仿真测试……6
6.5　实网测试……8
6.6　漏洞处置优先级评定……10
6.7　软件自主可控能力评定……11
附录 A（资料性）　资产库 ……13
附录 B（资料性）　组件库 ……14
附录 C（资料性）　漏洞库 ……15
参考文献 ……16

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。

本文件由中关村华安关键信息基础设施安全保护联盟提出并归口。

本文件起草单位：奇安信科技集团股份有限公司、软极网络技术（北京）有限公司、中国工业互联网研究院、可信华泰科技有限公司、北京大学、长沙市轨道交通运营有限公司、北京市科学技术研究院、中国移动通信集团有限公司、韶关学院、中共扬州市委网络安全和信息化委员会办公室、扬州市大数据管理中心、北京柏睿数据技术股份有限公司、浙江脑动极光医疗科技有限公司。

本文件主要起草人：刘立、郑新华、赵志娟、毛庆梅、张海彬、任燕、苗德成、栾浩、杜君、雷健波、刘如才、赵菁华、王舒、王喆、郑旻、段古纳、王珊珊、腾迪、王思登、孙可侻、刘先宝、郑国忠、王雪珊、严爱明、赵晶晶、韩月华、王晓怡、张坤。

引　言

软件产品自主可控能够有效规避停服断供或安插后门等安全隐患，对于确保国家在关键领域的独立性和安全性意义重大。加强对软件自主可控能力的测试管理，掌握当前的实际水平和潜在风险，是提升自主可控能力必不可少的措施。制定本团体标准，旨在规范软件研制单位、使用单位、测评机构的测试行为，提升其测试管理能力，确保软件自主可控能力的稳步提升。

本文件围绕软件自主可控能力测试方法进行深入剖析，主要包括两大部分，一是软件自主可控能力测试的管理框架，包括测试范围、管理粒度、测试框架以及如何基于网络靶场对测试过程和测试结果进行闭环管理。二是基于网络靶场开展软件自主可控能力测试的具体方法，首先要建立资产库、组件库、漏洞库等基础库，对软件资产信息进行初始化，然后结合软件生命周期阶段和安全管理需求开展静态测试、仿真测试和实网测试，对每种测试方法从制定测试方案、搭建测试环境、执行测试任务到输出测试报告给予详细的指导，根据测试结果评定漏洞处置优先级，并对软件自主可控能力进行判定。

本文件旨在帮助软件研制单位、使用单位、测评机构提升软件自主可控能力测试过程的科学性和严谨性，加强测试结果的连续性管理，进而提升对软件产品的技术掌控能力、持续交付能力和漏洞管理能力，为数字经济的健康发展提供有力支撑。

自主可控网络安全技术　基于网络靶场的软件自主可控能力测试指南

1　范围

本文件描述了一套基于网络靶场对软件自主可控能力进行持续性测试的方法论，包括在软件生命周期各阶段进行静态测试、仿真测试、实网测试时，如何制定测试方案、搭建测试环境、执行测试任务和输出测试报告。

本文件适用于指导组织基于网络靶场开展软件资产自主可控能力测评工作，能供软件产品研制单位、使用单位、测评机构等相关方参考使用。

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 20984—2022　信息安全技术　信息安全风险评估方法

GB/T 25069—2022　信息安全技术　术语

T/CSAC 001—2023　网络靶场　基于技战术模型的安全测评方法

T/ZISIA 01—2024　自主创新型网络安全技术　框架

3　术语和定义

GB/T 25069—2022 中界定的以及下列术语和定义适用于本文件。

3.1

自主可控　autonomous and controllable

产品在核心技术、原材料和零部件、生产工艺等方面不依赖于外部国家或公司，能够自主研发、生产、运营，并符合安全可控标准和监管要求。

3.2

安全可控　controllability for security

信息技术产品具备的保证其应用方的数据支配权、产品控制权、产品选择权等不受损害的属性。

[来源：GB/T 36630.1—2018，3.2]

3.3

软件资产　software asset

对组织有价值的软件资源，是自主可控测试的对象。

3.4

测试要素　test element

与测试活动相关的各种要素，包括但不限于测试目标、测试计划、测试人员、测试环境、测试方案、测试用例、测试工具和缺陷漏洞管理等。