ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 44862—2024

网络安全技术　网络弹性评价准则

Cybersecurity technology—Cyber-resilience evaluation criteria

2024-10-26 发布　　2025-05-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前言 …… Ⅲ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 1
5　概述 …… 2
5.1　网络弹性 …… 2
5.2　评价指标体系 …… 2
5.3　标准结构 …… 3
6　网络弹性指标 …… 3
6.1　预防能力 …… 3
6.1.1　态势感知 …… 3
6.1.2　检查分析 …… 4
6.1.3　协同防御 …… 4
6.1.4　供应链管理 …… 4
6.2　承受能力 …… 5
6.2.1　应急响应 …… 5
6.2.2　损失限制 …… 5
6.2.3　遏制 …… 5
6.2.4　生存性 …… 6
6.3　恢复能力 …… 6
6.3.1　灾难备份 …… 6
6.3.2　业务连续性 …… 6
6.3.3　数据与业务恢复 …… 7
6.4　适应能力 …… 7
6.4.1　自主管理 …… 7
6.4.2　重构 …… 8
6.4.3　节点适应性 …… 8
6.4.4　网络适应性 …… 8
7　评价方法 …… 9
附录 A（规范性）　网络弹性评价表 …… 10
附录 B（资料性）　极限场景、极端网络安全事件下网络弹性指标示例 …… 15
附录 C（资料性）　复杂信息系统网络弹性需求分析 …… 18
附录 D（资料性）　网络弹性架构设计方法 …… 20
参考文献 …… 26

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。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：大连理工大学、中国软件评测中心(工业和信息化部软件与集成电路促进中心)、国家工业信息安全发展研究中心、公安部第三研究所、中国科学技术大学、紫金山实验室、中国电子技术标准化研究院、联想(北京)有限公司、北京天融信网络安全技术有限公司、中国信息通信研究院、国家计算机网络应急技术处理协调中心、中国检验认证(集团)有限公司、国家信息技术安全研究中心、中国电信集团有限公司、中车大连机车车辆有限公司、天翼云科技有限公司、国电南京自动化股份有限公司、中能融合智慧科技有限公司、公安部第一研究所、华能信息技术有限公司、武汉金银湖实验室、华为技术有限公司、中兴通讯股份有限公司、信华信技术股份有限公司、中国烟草总公司湖北省公司、战略支援部队信息工程大学、东南大学、北京理工大学、深信服科技股份有限公司、陕西省信息化工程研究院、长扬科技(北京)股份有限公司、深圳开源互联网安全技术有限公司、嵩山实验室、安芯网盾(北京)科技有限公司、郑州昂视信息科技有限公司、网安联信息技术有限公司、广东云百科技有限公司。

本文件主要起草人：宋明秋、左晓栋、杨春立、黎水林、朱雪峰、张进、陈兴跃、上官晓丽、王惠莅、王冲华、李汝鑫、王少杰、于盟、卢春景、崔涛、喻梁文、王宝雁、刘亚天、呼博文、沈军、广小明、王大伟、朱良海、辛晨、刘文彪、黄石海、赵赫、汤成俊、赵硕、余果、汪慕峰、梁利、安宏杰、曹鲲鹏、潘中英、孙伟宏、杨斯可、宋景民、马海龙、曹向辉、郭泽华、赵晓荣、金伟、王语涵、谢琴、张亚京、王颉、张建辉、李天涯、李昂、伊玮珑、江文、阮懿宗、周柏魁。

网络安全技术　网络弹性评价准则

1　范围

本文件规定了网络弹性评价准则，给出了网络弹性评价指标体系和评价方法。

本文件适用于组织对网络弹性的自评价，网络安全服务机构对网络弹性的第三方评价，也适用于组织的网络弹性设计、建设和提升。

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 20988　信息安全技术　信息系统灾难恢复规范

GB/T 25069—2022　信息安全技术　术语

GB/T 30146—2023　安全与韧性　业务连续性管理体系　要求

GB/T 43269—2023　信息安全技术　网络安全应急能力评估准则

3　术语和定义

GB/T 25069—2022 界定的以及下列术语和定义适用于本文件。

3.1

网络弹性　cyber resilience

网络存在不利条件、压力、攻击或失陷组件时，自身所应具有的预防、承受、恢复和适应的能力，以保持系统功能和结构稳定，实现对重大网络安全事件的有序、有效应对，保证关键业务稳定运行。

注：本文件中术语“网络”指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

3.2

关键业务　critical business

一旦遭受网络安全事件可能严重影响组织或客户网络安全和稳定，造成重大损失的业务。

3.3

生存性　survivability

在攻击、失效、故障或中断发生的情况下，系统仍能运行基本业务功能，完成关键业务的能力。

注：失效是指一个系统或组件失去其设计所规定的目的或功能，尽管可以运行，但不能输出正确的结果。故障是指系统或设备不能执行规定功能的状态。基本业务功能是指组成业务功能的基本功能单元，如进程、线程或算法模块等。

[来源：ISO/IEC/IEEE 24765—2017，3.4060，有修改]

4　缩略语

下列缩略语适用于本文件。

API：接口（Application programming interface）