ICS 35.030
CCS L 70

团　　体　　标　　准

T/CIE 219—2024

信息安全技术　信息系统网络安全免疫框架　第4部分:免疫表征框架

Information security technology—Network security immunization framework for information systems—Part 4: Immunization representation framework

2024-03-20 发布　　2024-04-01 实施

中国电子学会　发布
中国标准出版社　出版

目　　次

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。

本文件是《信息安全技术　信息系统网络安全免疫框架》的第4部分。已经发布了以下部分:

——第1部分:概述;

——第2部分:基因鉴别框架;

——第3部分:免疫识别框架;

——第4部分:免疫表征框架;

——第5部分:免疫控制框架。

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。

本文件由中国电子学会提出归并口。

本文件起草单位:四川大学、成都信息工程大学、深圳大学、北京邮电大学。

本文件主要起草人:李涛、兰小龙、李汶珊、李贝贝、何俊江、刘翱、麻文刚、黄继武、谢宁、刘晓洁、赵辉、彭海朋、陈昌盛、李昊东、王宏霞、方文波、马欣蕾。

引　言

当前，全球网络安全正在迈入未知威胁频发的新时代。信息系统网络安全免疫技术以模拟人体免疫系统的机制为核心，旨在实现信息系统的身份验证、威胁检测、风险评估与控制，并通过构建具备自我演化进化能力的网络安全体系，及时识别未知威胁及已知威胁的变种，有效应对复杂多变的网络攻击与威胁，适应当今动态多样的网络环境，构建更加智能、灵活的安全防护体系。

然而，我国在网络安全免疫领域的研究尚处于起步阶段，相关概念、术语和技术规范仍不统一，这在一定程度上制约了技术的深入发展和应用推广。推动网络安全免疫技术的体系化建设，已成为提升我国网络安全能力的迫切需求。《信息安全技术　信息系统网络安全免疫框架》系列标准旨在确立适用于网络安全免疫相关标准化文件的起草、制定和组织工作的原则，拟由五个部分构成。

——第 1 部分：概述。目的在于明确信息系统网络安全免疫的基本概念、术语和技术规范。

——第 2 部分：基因鉴别框架。目的在于明确基因鉴别的基本概念、目标、方案、框架与流程。

——第 3 部分：免疫识别框架。目的在于明确免疫识别的基本概念、目标、方案、框架与流程。

——第 4 部分：免疫表征框架。目的在于明确免疫表征的基本概念、目标、方案、框架与流程。

——第 5 部分：免疫控制框架。目的在于明确免疫控制的基本概念、目标、方案、框架与流程。

免疫表征旨在通过模拟人体免疫系统的发烧预警机制，对信息系统网络实现实时、定量、准确的快速评估，对提高未知威胁以及已知网络威胁变种的预警能力至关重要。因此，编制本文件尤为必要。

信息系统网络安全免疫相关技术标准的制定，对推动我国网络安全科学技术实现跨越式发展，对我国推动网络安全免疫领域的科学研究、人才培养和产业进步具有重要作用。

信息安全技术　信息系统网络安全免疫框架　第4部分:免疫表征框架

1　范围

本文件规定了信息系统网络安全免疫表征框架内容,包括:

——定义了信息系统网络安全免疫表征的相关术语和基本概念;

——定义了信息系统网络安全免疫表征功能与免疫表征要素之间的关系;

——定义了信息系统网络威胁免疫表征的实施流程和方法。

本文件也规定了网络威胁免疫表征的基本概念、网络威胁免疫表征要素关系、网络免疫表征的实施流程和方法。

本文件适用于信息系统网络安全免疫表征工作。

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 25069　信息安全技术　术语

T/CIE 218—2024　信息安全技术　信息系统网络安全免疫框架　第3部分:免疫识别框架

3　术语和定义

GB/T 25069 和 T/CIE 218—2024 界定的以及下列术语和定义适用于本文件。

3.1

网络威胁基因　network threat genes

通过提取当前网络威胁的典型风险特征,并将这些特征编码形成一种独特的识别序列。

3.2

血亲关系　consanguinity relationship

在一个集合中,如果两个元素的基因具有相似性,则称这两个元素具有血亲关系。

注:在本文件中,若非特别说明,血亲关系一般系指检测器中的血亲关系。

3.3

血亲类　consanguinity class

在一个集合中,所有元素之间均具有血亲关系的集合。

注:在本文件中,若非特别说明,血亲类一般系指检测器中的血亲类。

3.4

最大血亲类　maximal consanguinity class

一个血亲类不真包含于任何其他血亲类的集合。

注:在本文件中,若非特别说明,最大血亲类一般系指检测器中的最大血亲类。