ICS 35.030
CCS L 70

团　　体　　标　　准

T/CIE 217—2024

信息安全技术　信息系统网络安全免疫框架　第2部分:基因鉴别框架

Information security technology—Network security immunization framework for information systems—Part 2: Genetic identification 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2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并归口。

本文件起草单位：四川大学、中国科学院信息工程研究所、成都信息工程大学、北京大学、数据通信科学技术研究所。

本文件主要起草人：李涛、李汶珊、李贝贝、兰小龙、何俊江、刘翱、麻文刚、林东岱、王文浩、刘晓洁、赵辉、王平、周斌、黄致程、周建群、赵奎、朱子青、简欣娅、于楠、黄震宇、王宏霞、戴婉莹、黄翰媛、李佳琦、邵泽瑞、杜卿云、于帆、杨贺昆。

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。

基因鉴别旨在建立一种基于基因关系的身份合法性验证机制，以确保网络中的实体可以互相信任，对实现信息系统的高效访问控制能力至关重要。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2部分:基因鉴别框架

1　范围

本文件规定了信息系统网络安全免疫框架中的基因鉴别框架,包括:

a)　确定基因鉴别框架下的术语和定义;

b)　定义基因鉴别的基本概念、基因鉴别的目标;

c)　制定基因鉴别方案、基因鉴别框架与基因鉴别流程。

本文件适用于信息系统的基因鉴别工作。

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

3　术语和定义

GB/T 25069界定的以及下列术语和定适用于本文件。

3.1

网络成员　network member

网络中的元素,可以是网络服务、应用程序、服务器、设备、用户等。

3.2

网络家族　network family

网络中不同网络成员之间的一个从属关系,网络成员按照从属关系构成一个树状图谱,整棵树被称为一个家族,树的根节点又称为网络始祖,表明其下属所有网络成员均由其演化而来。

注:与树的概念类似,网络家族的定义也是递归的,即网络家族图谱树中的一子树又被称为一个子网络家族。

3.3

网络家族成员　network family member

网络成员的一种,指网络家族图谱中的每一个节点,包括祖先、父亲、兄弟、子女等,其中父节点连同其下一级节点(子女)构成一个家庭,该父节点又被称为该家庭的家长。

3.4

网络成员基因　network member gene

网络家族成员的特定特征或属性的编码序列,用于标明其在网络家族中的身份,对外公开,包含两部分:家族基因和个体基因,其中家族基因是其父亲的基因,个体基因是成员在家庭中的唯一编码。

注:若父辈系网络始祖,则其成员基因由自身决定,可以为空。