联盟技术规范《信息安全技术 网络安全产品互联互通 告警信息格式》（征求意见稿）编制说明

一、工作简况

1．任务来源

2022年7月，中国网络安全产业联盟在中央网信办网络安全协调局的指导和要求下成立了网络安全产品互联互通工作组，推动网络安全产品互联互通建设。

2022年7月，中国网络安全产业联盟网络安全产品互联互通工作组经组内征集，联盟技术规范《信息安全技术 网络安全产品互联互通 告警信息格式》由国家信息中心牵头编制，该规范由中国网络安全产业联盟归口管理。

2．编制的主要成员单位

本规范由国家信息中心主要负责编制，中国电子技术标准化研究院、国家互联网应急中心、中国科学院信息工程研究所、杭州安恒信息技术股份有限公司、深信服科技股份有限公司、北京天融信网络安全技术有限公司、北京神州绿盟科技有限公司、东软集团股份有限公司、北京升鑫网络科技有限公司、安天科技集团股份有限公司等单位共同参与了该规范的起草工作。

3．主要工作过程

自 2021 年下半年以来，中国网络安全产业联盟在中央网信办网络安全协调局指导下，组织国家互联网应急中心等行业用户，和天融信等网络安全骨干企业开展了网络安全产品互联互通前期基础研究工作，初步形成互联互通工作思路与框架体系，对资产信息格式在内的六项互联互通信息和安全防护等四项互联互通功能进行整体规划。

2022 年 7 月，中国网络安全产业联盟在中央网信办网络安全协调局的指导和要求下成立了网络安全产品互联互通工作组，工作组将互联互通资产信息格式和告警信息格式两项技术规范列为急需研制的重点标准项目。经工作组组内征集，本规范由国家信息中心负责牵头编制，规范的编制组包括国家互联网应急中心等用户单位和天融信、深信服、安恒、绿盟、东软等安全厂商。

2022 年 8 月至 9 月中旬，编制组充分考虑各行业客户对资产管理的需求，结合实际项目工程经验，参考国内外相关标准，编制完成规范草案；

2022 年 9 月中旬至 10 月底，经编制组组内多次会议研讨，并邀请业界专家多次会议

评审和函审，形成规范草案第二版；

2022 年 11 月至 2023 年 3 月，联盟组织行业用户和安全企业开展本规范的试点验证；

2023 年 4 月上旬，编制组根据试点验证过程中各试点单位提出的意见建议，对规范进行修改完善，形成规范征求意见稿。

二、编制原则，和确定主要内容的论据及解决的主要问题

1．制定的基本原则

本规范的编制原则是：

1）通用性

本规范拟提出统一的互联互通告警信息格式，指导厂商、用户单位等开展网络安全产品互联互通建设工作，降低不同安全厂商、安全产品的适配成本。

2）实用性

根据我国国情、实际应用环境和国家有关政策编制本规范，使其在指导用户单位与安全厂商互联互通建设过程中具有很强的实用性。

3）可行性

在规范研制过程中，根据规范技术内容成熟度情况依托中国网络安全产业联盟推动相关单位开展试点验证工作，确保规范条款的可行性。

4）一致性

符合国家相关法律法规与政策文件，并于现行标准规范协调一致。

2．确定主要内容的依据

本规范制定的依据为：

a）规范格式按照GB/T 1.1—2020标准要求编写。

b）本规范制定参考以下政策文件与国家标准：

《中华人民共和国网络安全法》

《关键信息基础设施安全保护条例》

《“十四五”国家信息化规划》

《国家网络安全事件应急预案》

GB/T 28458-2020《信息安全技术 网络安全漏洞标识与描述规范》

GB/T 28517-2012《网络安全事件描述和交换格式》

GB/T 36643-2018《信息安全技术 网络安全威胁信息格式规范》

GB/T 37027-2018《信息安全技术 网络攻击定义及描述规范》

GB/T XXXX-XXXX《信息安全技术 网络安全产品互联互通框架》（征求意见稿）

3．解决的主要问题

近年来，《网络安全法》《关键信息基础设施安全保护条例》《“十四五”国家信息化规划》等法律法规、政策文件陆续出台，对建立跨部门、跨行业高效联动的网络安全防护能力提出了新的要求。智能化、自动化的协同防护能力建设依赖于不同网络安全产品的互联互通。然而，当前我国网络安全产品互联互通仍在起步阶段，大量研发成本用于实现不同安全厂商、安全产品之间的适配，用户单位互联互通工作改造成本高、效果不明显，急需出台标准指导相关工作开展。

本规范在研制过程中调研了国内外网络安全产品互联互通相关政策法规、标准规范与技术实现，对现有政务、电信、金融等行业用户单位和国内主流安全厂商互联互通实践情况与互联互通需求进行了分析。根据现有互联互通实践与互联互通实际需求，根据我国实际情况拟提出统一的互联互通告警信息格式，指导用户单位、厂商等开展网络安全产品互联互通工作，拟解决当前网络安全产品难以有效联通，网络安全信息难以高效、大范围共享的问题。

本规范主要框架如下：

前言

第 1 章 范围

规定了网络安全产品告警信息的描述格式。

适用于网络安全产品互联互通功能的设计、开发、应用和测试。

第 2 章 规范性引用文件

GB/T 25069-2022 信息安全技术 术语

GB/Z 20986-XXXX 信息安全技术 网络安全事件分类分级指南

GB/T AAAAA.1-20XX 信息安全技术 网络安全产品互联互通框架

第 3 章 术语和定义

GB/T 25069-2022、GB/T AAAAA.1-20XX 界定的以及下列术语和定义适用于本文件。

3.1 告警 alert

网络安全产品依据设定的规则或模型，对采集到的网络安全要素进行规则匹配，以及经过归并或聚合分析后，自动产生的风险警示信息。

第 4 章 告警分类

告警信息可分为恶意程序告警、网络攻击告警、数据安全告警、异常行为告警和其他告警 5 类，每个基本分类分别包括若干个子类。

4.2-4.6 章给出了 5 类告警的描述。

第 5 章 告警信息数据格式

告警信息的数据格式由通用部分、告警分类专用部分组成，专用部分由分类基础信息（如有）和告警子类扩展信息（如有）共同组成。

注：以恶意程序告警中的计算机病毒告警为例，计算机病毒告警的完整数据格式为：告警通用部分（表 2）+恶意程序告警基础信息格式（表 3）+计算机病毒告警扩展信息格式（表 4）。

5.2 给出了告警信息数据字段类型的取值，5.3 给出了告警信息通用部分格式，5.4 给出了告警信息专用部分格式。

本规范中的附录均为规范性附录，其中附录 A 给出了网络安全产品互联互通告警信息分类代码，附录 B 给出了网络安全设备类型编码。

三、主要试验[或验证]情况分析

2022年11月，根据规范初步形成了告警信息描述技术方案，依托中国网络安全产业联盟，组织国家信息中心、国家互联网应急中心、中国科学院信息工程研究所、北京天融信网络安全技术有限公司、深信服科技股份有限公司、杭州安恒信息技术股份有限公司、绿盟科技集团股份有限公司、东软集团股份有限公司、安天科技集团股份有限公司、北京升鑫网络科技有限公司等共10家单位开展告警信息格式试点验证。

根据各试点单位反馈，经过统计，告警信息相关的35项条款中适用性均超过50%，规范条款基本能够覆盖现有网络安全产品互联互通过程中应提供的数据，表明规范条款在实际业务场景中可落地可实施，按照本规范开展的网络安全产品互联互通建设工作具有一定通用性、可行性与实用性。

四、专利情况说明

本规范不涉及专利及知识产权问题。

五、产业化情况、推广应用论证和预期达到的经济效果

目前，我国政务、电信、金融等行业用户单位及国内主流安全厂商均已开展网络安全产品互联互通实践工作，各行业各企业对于网络安全产品互联互通标准的需求明显。网络

安全产品告警信息格式能够指导网络安全产品互联互通功能的设计、开发、应用和测试，降低安全厂商、安全产品的之间的适配成本，降低用户单位互联互通工作改造成本，提升互联互通工作建设效果。

六、与现行相关法律、法规、规章的协调性

本规范与现行法律、法规、强制性国家标准及相关标准协调一致。本规范在同《中华人民共和国网络安全法》《关键信息基础设施安全保护条例》《“十四五”国家信息化规划》《国家网络安全事件应急预案》等相关法律法规和政策文件及现行国家标准GB/T 28458-2020《信息安全技术 网络安全漏洞标识与描述规范》、GB/T 28517-2012《网络安全事件描述和交换格式》、GB/T 36643-2018《信息安全技术 网络安全威胁信息格式规范》、GB/T 37027-2018《信息安全技术 网络攻击定义及描述规范》协调一致基础上，在研制过程中引用了GB/T 20986-XXXX《信息安全技术 网络安全事件分类分级指南》（报批稿）、GB/T 25066-2020《信息安全技术 信息安全产品类别与代码》、GB/T 30279-2020《信息安全技术 网络安全漏洞分类分级指南》、GB/T XXXX-XXXX《信息安全技术 网络安全产品互联互通框架》（征求意见稿）相关内容，针对网络安全产品互联互通应用提出具体要求。

七、重大分歧意见的处理经过和依据

无。

八、贯彻联盟技术规范的要求和措施建议

本规范主要用于指导网络安全产品互联互通功能的设计、开发、应用和测试，建议计划开展网络安全产品互联互通建设的用户单位、安全厂商等依据本规范给出的网络安全产品互联互通告警信息格式开展产品互联互通工作。

九、其他应予以说明的事项

无。

《信息安全技术 网络安全产品互联互通 告警信息格式》编制工作组

2023-04-14