ICS 35.240.40
CCS A 11

中华人民共和国国家标准

GB/T 42708—2023

金融网络安全威胁信息共享指南

Guideline for financial cybersecurity threat information sharing

2023-08-06 发布　　2023-08-06 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

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。

本文件由全国金融标准化技术委员会(SAC/TC 180)归口。

本文件起草单位：北京银联金卡科技有限公司、中国工商银行股份有限公司、中国建设银行股份有限公司、建信金融科技有限责任公司、中国邮政储蓄银行股份有限公司、中国银联股份有限公司、中国银行股份有限公司、中国农业银行股份有限公司、联通支付有限公司、天翼电子商务有限公司、北京国家金融科技认证中心有限公司、腾讯云计算(北京)有限责任公司。

本文件主要起草人：王玲、李晓伟、张志波、于鸽、李博文、段超、侯晓晨、余思、聂玉涵、陈德锋、黄建德、廖渊、赵凯峰、苏涵、王美科、何启翱、刘汝隽、任震、彭大祥、孟熹、潘丽扬、李凡、蒋增增、林智鑫。

引　言

当前，互联网技术在金融行业广泛应用，网络技术既给广大用户带来便利，又带来网络安全威胁。金融行业增强网络安全威胁信息的获取能力，强化威胁信息共享和使用，有助于提升网络安全防控整体水平。

金融网络安全威胁信息共享旨在采用技术手段实现网络安全威胁信息的有效流动，通过建立威胁信息共享机制，促进威胁信息的融合、分析，提升威胁信息利用的精准度，实现安全风险的及时预警、响应和处置，以降低金融网络威胁信息的使用成本，提升金融网络风险处置能力。

金融网络安全威胁信息共享指南

1 范围

本文件给出了金融网络安全威胁信息的共享框架、共享原则、共享方式、共享流程、质量管理、保障机制、安全管理等方面的建议。

本文件适用于参与金融网络安全威胁信息共享的金融机构和相关组织。

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 2260 中华人民共和国行政区划代码

GB/T 2659 世界各国和地区名称代码

GB 32100 法人和其他组织统一社会信用代码编码规则

3 术语和定义

下列术语和定义适用于本文件。

3.1

威胁 threat

可能对系统或组织造成危害的不期望事件的潜在原由。

[来源：GB/T 29246—2017，2.83]

3.2

威胁信息 threat information

一种基于证据的知识，用于描述现有的或可能出现的威胁，从而实现对威胁的响应和预防。

注：威胁信息包括上下文、攻击机制、攻击指标、可能影响等信息。

[来源：GB/T 36643—2018，3.3]

3.3

威胁信息控制者 threat information controller

有能力决定威胁信息处理目的、方式等的组织或个人。

3.4

共享 sharing

威胁信息控制者向其他控制者提供威胁信息，且双方分别对威胁信息拥有独立控制权的过程。

4 缩略语

下列缩略语适用于本文件。

API：应用程序接口(Application Programming Interface)