ICS 35.030
CCS L80

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术　关键信息基础设施网络安全应急体系框架

Information security technology — Framework for cybersecurity emergency system of critical information infrastructure

（征求意见稿）

（本稿完成日期：2022 年 11 月 9 日）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX — XX — XX 发布　　XXXX — XX — XX 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。

本文件由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本文件起草单位：腾讯科技（北京）有限公司、国家工业信息安全发展研究中心、中国信息通信研究院、中国电子技术标准化研究院、国家计算机网络应急技术处理协调中心、公安部第三研究所、中国网络安全审查技术与认证中心、国家应急管理部大数据中心、国家能源局信息中心、中国移动通信集团有限公司、华为技术有限公司、阿里云计算有限公司、北京百度网讯科技有限公司、中国科学院信息工程研究所、国家信息中心、国家信息技术安全研究中心、中国工业互联网研究院、中国软件评测中心、中国交通通信信息中心、国家计算机网络应急技术处理协调中心云南分中心、陕西省网络与信息安全测评中心、北京快手科技有限公司、北京天融信网络安全技术有限公司、成都卫士通信息产业股份有限公司、北京路云天网络安全技术研究院有限公司、北京升鑫网络科技有限公司。

本文件主要起草人：秦小伟、龚斌、郭臣、于盟、陈亮、孟楠、舒敏、王惠莅、李雪莹、吴波、落红卫、王婷、王文磊、陈悦、任卫红、袁静、杜红亮、孙晓丽、韩言妮、邱勤、史波良、鲍文平、李沛林、魏玉峰、黄玉钏、吴桐、董健、李安伦、张哲宇、韩晓露、应志军、李焕、王国宇、毕钰、王二州、王海棠、韩冬旭、赵呈东、卜哲、鲍旭华、陈蕾、王龑、李亚玲、王诗蕊。

信息安全技术　关键信息基础设施网络安全应急体系框架

1　范围

本文件给出了关键信息基础设施网络安全应急体系框架，包括机构设立、分析识别、应急预案、监测预警、应急处置、事后恢复与总结、事件报告与信息共享、应急保障、演练与培训。

本文件适用于关键信息基础设施运营者建立健全网络安全应急体系、开展网络安全应急活动，也可供关键信息基础设施安全保护的其他相关方参考。

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/Z 20986　信息安全技术　信息安全事件分类分级指南

GB/T 25069—2022　信息安全技术　术语

GB/T 39204—2022　信息安全技术　关键信息基础设施安全保护要求

GB/T AAAAA—XXXX　信息安全技术　网络安全信息共享指南

3　术语和定义

GB/T 25069—2022 和 GB/T 39204—2022 界定的以及下列术语和定义适用于本文件。

3.1

关键信息基础设施　critical information infrastructure

公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

[来源：GB/T 39204—2022，3.1]

3.2

网络安全事件　cybersecurity incident

由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据和业务应用造成危害，对国家、社会、经济造成负面影响的事件。

[来源：GB/T 38645—2020，3.1]

3.3

应急响应　emergency response

为了应对网络安全事件发生所做的准备，以及在网络安全事件发生后所采取的措施。

[来源：GB/T 24363—2009，3.4，有修改]

3.4

应急预案 emergency plan

为了应对网络安全事件而编制的，对关键信息基础设施进行维持、恢复，保障关键业务安全稳定运行的策略和规程。

3.5

网络安全应急相关方 cybersecurity emergency relevant party

负责、参与关键信息基础设施网络安全保护和应急活动的有关实体。

3.6

供应链 supply chain

将多个资源和过程联系在一起，并根据服务协议或其他采购协议建立连续供应关系的组织系列。

[来源：GB/T 39204—2022，3.2]

3.7

关键业务链 critical business chain

组织的一个或多个相互关联的业务构成的关键业务流程。

[来源：GB/T 39204—2022，3.3]

4 缩略语

下列缩略语适用于本文件。

CII：关键信息基础设施（critical information infrastructure）

5 总体架构

CII运营者首先设立专门安全管理机构，统筹负责本单位网络安全应急工作，依据对关键业务分析识别结果，制定本单位网络安全应急预案。在网络安全事件发生前，通过技术监测、情报收集等手段，发现CII面临的网络安全威胁，及时消除风险并降低发生网络安全事件的概率；在网络安全事件发生时，启动应急预案，快速定位问题并终止紧急状态；在网络安全事件得到控制后，开展后期处置，将CII恢复到事前运行状态并进行总结分析。

CII运营者发现网络安全事件或威胁时，按要求通过信息共享接口及时向国家网信部门、保护工作部门、公安机关和网络安全服务机构等共享信息；发生重大网络安全事件时，按要求通过事件报告接口向国家网信部门、保护工作部门和公安机关报告。

CII网络安全应急体系框架的总体架构见图1。

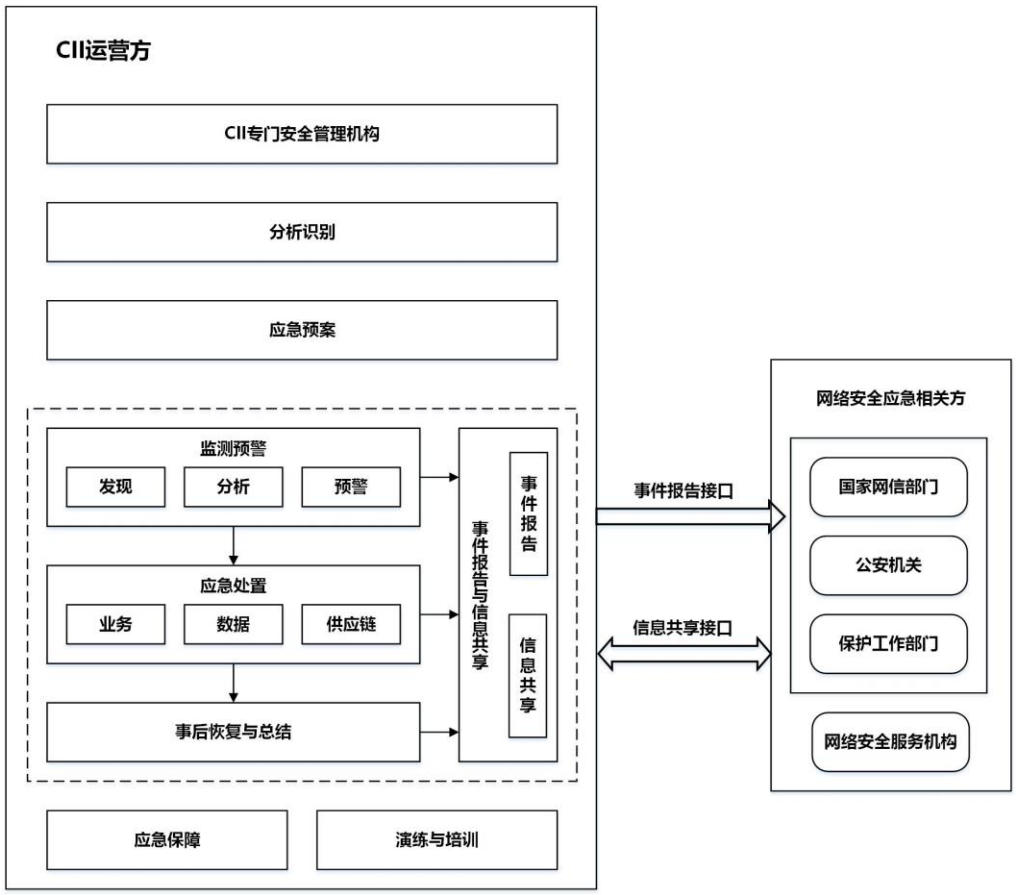

图1 关键信息基础设施网络安全应急体系框架

6 机构设立

CII运营者设立专门安全管理机构，机构的领导由CII运营者最高管理层的分管领导担任，成员包括各相关部门负责人、技术支撑人员、咨询专家和对内、对外联络人员等。CII专门安全管理机构的职责包括：

a）统筹协调，负责领导和决策本单位CII网络安全应急事项，在发生网络安全事件期间负责指挥协调；

b）制定应急预案，依据分析识别结果，制定网络安全应急预案；

c）监测预警，负责组织常态化网络安全监测，及时发现CII面临的网络安全风险或威胁，并及时预警；

d）事件报告，负责对接国家网信部门、保护工作部门和公安机关，落实重大网络安全事件报告要求；

e）信息共享，负责对内、对外联络，落实网络安全信息共享要求；

f）应急处置，负责组织现场应急处置；

g）应急保障，负责落实物资、人力、资金等保障事项。

7 分析识别

CII运营者需要对关键业务进行分析识别，确定本单位关键业务运行情况以及对外部业务的依赖性、重要性，以支撑编制网络安全应急预案、开展网络安全应急活动。

a）基本情况梳理

梳理关键业务的服务对象、地域分布、组织结构、管理模式、岗位设置等，明确关键业务的运行特征、业务逻辑、运行架构、业务范围，确定关键业务的基本功能。

b）关键业务链识别

梳理与本单位关键业务相关联的外部业务，识别支撑关键业务的CII分布、运营情况，确定对外部业务的依赖性、重要性。

c）CII数据识别

分析关键业务在收集、存储、使用、加工、传输、输出、共享等环节中涉及到的数据情况，如配置数据、运行数据、业务数据、用户数据等，明确数据的种类、作用，形成CII数据清单。

d）重要资产识别

识别关键业务安全稳定运行不可或缺的网络设施、信息系统等重要资产，厘清上述网络设施、信息系统的功能作用、结构组成、网络拓扑、地理位置以及与关键业务之间的支撑作用、依赖关系，形成CII资产清单。

e）供应链识别

识别CII资产所依赖的重要零部件、服务等信息，确定主要供货商，形成CII供应链清单。

8 应急预案

CII运营者以关键业务为核心制定网络安全应急预案。

a）在国家网络安全事件应急预案的框架下，CII专门安全管理机构组织技术、安全、业务、运维、采购等部门，建立健全本单位网络安全应急预案体系，包括总体应急预案、专项应急预案，规定统一的应急预案框架，明确应急预案的适用范围、启动预案的条件等；

b）应急预案要素需要齐全，包括确定组织机构职责，基于分析识别的结果，明确监测预警、应急处置、事后恢复与总结、事件报告和信息共享的实施方法，明确应急保障、演练与培训的落实细节；

c）明确应急策略，在应急预案中明确，一旦网络设施、信息系统受到损害或者发生故障时，需要维护的关键业务功能，并明确遭受破坏时恢复关键业务的时间；

d）根据关键业务对连续性、安全性的不同要求，在应急预案中明确重要资产功能的恢复顺序、处置方法，包括非常规时期、遭受大规模攻击时等处置流程；

e）根据网络安全事件的类型、敏感程度以及对业务的影响范围等因素，在应急预案中确定事件分级、预警分级和响应分级的标准，并与上位预案相衔接；

f）网络安全应急预案需要有联系方式清单，包括应急值班24小时联系电话、重要资产责任人联系方式、专家名单与联系方式、网络安全应急技术队伍联系方式、应急相关方联系方式等；

g）制定应急预案操作手册，明确培训内容、频率、方式和对象；

h）制定应急演练手册，明确演练频率、组织方式和演练形式，评价预案内容的针对性、实用性和可操作性，实现应急预案的科学管理和优化更新。

9 监测预警

9.1 风险发现

CII运营者在风险发现方面：

a）建设网络安全监控中心，开展7*24h安全监测，监测内容需要包括网络流量、日志信息、运行状态、性能状况和异常行为等；

b）具备2种以上威胁信息收集渠道，收集内外部网络安全威胁信息，包括内部报告的安全隐患、可疑事件和外部发布的安全漏洞、网络攻击最新动态等；

c）每年至少开展一次网络安全检测和风险评估，发现CII面临的风险和威胁；

d）留存重要监测数据时间不少于6个月，并符合国家、行业或地方有关部门网络安全应急相关法规的要求。

9.2 风险分析

CII运营者在风险分析方面：

a）装备分析工具、制定分析方法，全面分析日志、流量、漏洞和恶意代码；

b）制定威胁模型，挖掘检测规避、隐蔽通信、数据加密、欺骗绕过等高级网络攻击行为；

c）制定多源异构数据、多业务场景分析方法，分析无文件攻击、供应链攻击、账户凭据盗用等深层网络安全风险；

d）制定多源信息融合分析方法，综合研判CII业务、数据和供应链面临的网络安全态势；

e）按照GB/Z 20986对网络安全事件实施分级分类。

9.3 风险预警

CII运营者在风险预警方面：

a）制定内部预警通报制度，对发现或发生的风险、威胁，及时在内部发出预警；

b）根据不同等级、不同类别的网络安全事件制定相应的预警响应措施；

c）通过多种渠道及时采集内外部网络安全信息，并持续跟踪网络安全信息的变化情况，适时调整预警响应措施；

d）对于发现的可能造成较大影响的网络安全威胁信息，及时向保护工作部门、公安机关报告，并根据网络安全威胁信息的变化情况，及时补报最新网络安全威胁信息。

10 应急处置

10.1 概述

CII运营者需要组建专业应急处置队伍，建立网络安全应急响应机制，确保危害CII业务、数据和供应链的事件得到及时处置，保障关键业务安全稳定运行。

10.2 应急处置机制

CII运营者网络安全应急响应机制包括：

a）建设网络安全应急指挥中心，制定指挥调度规范流程，实施7*24h值班值守；

b）制定抑制、根除、恢复网络安全事件和威胁的方法；

c）针对网络攻击活动，制定应对方案，分析攻击路线、攻击目标，采取捕获、干扰、阻断、封控、加固等手段，快速切断攻击路线；

d）部署自动化安全响应和自动实施封禁技术，如自动隔离有害程序事件、自动阻止网络攻击事件等；

e）制定协同处置方案，在国家网信部门、保护工作部门和公安机关的指导下，开展或配合网络安全事件处置工作；

f）密切关注事件舆情，并根据国家网信部门、保护工作部门和公安机关要求向社会公众通告网络安全事件情况以及避免或减轻危害的措施，及时消除舆情；

g）对于未知类型的网络安全事件，根据影响情况果断采取措施，最大可能降低事件影响；

h）按要求，对网络攻击进行溯源、取证。

10.3 业务应急处置

CII运营者针对业务瘫痪情况，制订业务专项应急处置措施，具体内容包括：

a）针对带宽需求激增、网络可用性受限等情况，紧急提升网络容量，满足业务运行对网络带宽的需求；

b）针对业务运行中断的情况，启用备用网络设施、信息系统或者在多个备份点之间临时转移业务负载；

c）针对办公场所遭到网络攻击或者遭受火灾、水灾、地震等灾害时，临时切换工作场所或采用线上办公。

10.4 数据应急处置

CII运营者针对数据被篡改、违规使用或者滥用、泄露（丢失）和被损毁等各类数据安全事件场景，制定数据专项应急处置措施，包括：

a）针对数据被篡改的情况，分析攻击来源、攻击路径，针对性反制或抑制网络攻击，防止数据继续被篡改；

b）针对数据违规使用或者滥用情况，及时发布权威信息，消除数据违规使用或者滥用产生次生危害；

c）针对数据泄露（丢失）的情况，及时下线或切断相关业务系统外联网络，防止数据继续泄露（丢失）；

d）在数据被损毁时，从最近有效的备份中紧急恢复数据，保障业务运行需要。

10.5 供应链应急处置

CII运营者针对在网络安全事件期间供应链风险，制定专项应急处置措施：

a）密切跟踪供应链受安全事件干扰和危害情况，及时有效的调节应对措施，降低事件影响并防止进一步蔓延；

b）按照网络安全事件发展情况，及时向供应链供货商共享与其相关的安全信息，获得必要的信息、技术等方面的支持；

c）与供应链供货商紧急联系，确保在网络安全事件发生期间可以得到必需的零部件供应，避免供应链中断。

11 事后恢复与总结

CII运营者对于事后恢复与总结：

a）按照先应急处置、后恢复的原则，在网络安全事件得到控制以后，及时将关键业务、网络设施、信息系统恢复到事件之前的运行状态；

b）针对未知类型的网络安全事件，要详细记录处置过程、事件细节、事件发展趋势、处置经验等相关信息；

c）妥善保存网络访问日志、物理访问日志、审计日志等，以备溯源和调查取证；

d）对关键业务、网络设施、信息系统的恢复情况进行评估，查找事件原因，并采取措施防止再次发生同类事件；

e）对应急处置过程进行总结，分析应急处置过程中是否存在需要完善的环节，并根据分析结果优化应急预案；

f）在事件得到妥善处理后，形成完整的事件处理报告。

12 事件报告与信息共享

12.1 事件报告

CII运营者在事件报告方面：

a）针对特别重大网络安全事件、重大网络安全事件，按要求及时向保护工作部门、公安机关报告，简要说明事件发生的时间、危害情况和采取的措施；

b）在事件得到妥善处置后，按要求向保护工作部门、公安机关提交详细事件报告，包括事故发生时间、终止时间、发生地点、起因、影响范围、应急处置情况、事后恢复情况、应对经验以及采取的防范措施等；

c）在重大活动期间，按照要求实施“边处置、边报告”。

12.2 信息共享

12.2.1 信息共享机制

CII运营者依据GB/T AAAAA—XXXX制定本单位网络安全信息共享制度，及时向相关方共享CII网络安全信息。

a）按要求向国家网信部门、保护工作部门和公安机关等国家主管部门及时共享网络安全信息；

b）运营者可以根据本单位实际情况，与同一CII的其他运营者、关键业务链紧密相关的上下游运营者、网络安全服务机构、科研机构、业界专家等之间建立信息共享渠道和合作机制；

c）当网络安全共享信息为漏洞信息时，需要符合国家关于漏洞管理制度的要求；

d）持续跟踪事态变化情况，及时共享最新网络安全事件信息；

e）定期对网络安全信息共享模式、方法进行评估并持续改进。

12.2.2 信息共享内容

共享信息内容参照GB/T AAAAA—XXXX，其中与网络安全事件相关的信息可包括：

a） 事件描述信息

描述网络安全事件的信息，包括事件的起始时间、涉及对象、现象、攻击原理、影响范围等。

b） 攻击者描述信息

描述攻击者的动机、能力等相关的信息，包含攻击者的意图、与目标对象的利益关系、攻击者能使用的手段和方法等。

c） 应对经验信息

描述实施网络安全威胁行为主体的历史行为，以及在网络安全防护和网络安全事件响应等方面积累的成功经验和失败教训等。

d） 应对措施信息

描述对网络安全事件已实施的防御措施和处置措施等。

e) 其他信息

如最佳实践、前沿技术等。

13 应急保障

13.1 基础保障

CII运营者在基础保障方面：

a）落实网络安全应急资源，包括通信、电力、物资、人力等方面的需求，确保一旦发生网络安全事件时，应急响应活动所须的人、财、物等基本条件得到保障；

b）持续加强技术能力和技术队伍建设，不断提升在应急管理规划、监测预警、事件分析、应急处置、数据备份、系统恢复、调查取证等方面的技术能力。

c）妥善管理应急工具、装备、设施，及时对软硬件进行升级维护，确保应急工具装备、备品备件充足有效，确保应急设施随时可用。

13.2 协同保障

CII运营者在协同保障方面：

a）保障本单位信息共享机制正常运行，确保安全信息、威胁信息、预警信息和指挥协调信息等正常流通；

b）确保制度、技术等方面符合国家有关规定，确保对安全漏洞、安全威胁、入侵攻击、异常行为等进行协同处置时不发生技术冲突；

c）可以通过成立联合工作组、组建联合应急处置队伍等方式，强化组织间合作，提高应对网络安全事件的水平和协同配合能力。

13.3 业务保障

CII运营者在业务保障方面：

a）采用动态网络管理技术，实现网络容量弹性化，应对网络安全事件发生期间带宽需求激增、可用性受限的情况；

b）采用多模备份方案，针对关键业务安全稳定运行不可或缺的重要网络设施、信息系统，宜实施“双节点”备份，或将关键业务托管到不同的云平台上，在紧急情况下具备在备份点之间转移业务的能力；

c）定期对关键业务的信息化建设、信息化管理和信息化运行情况进行梳理，确保网络安全监测范围覆盖关键业务的整个信息化部分，及时发现并处理风险；

d）定期开展分析识别，及时更新CII资产清单，确保容灾备份清单真实、有效。

13.4 数据保障

CII运营者在数据安全保障方面：

a）对CII数据实施分类分级管理，制定重要数据和核心数据目录台账，针对不同类型数据制定相专项护措施；

b）建立数据备份机制，重要数据异地备份；

c）加强在收集、存储、使用、加工、传输、输出、共享等关键环节的数据保护措施，采取加密、脱敏、去标志化等手段保护敏感数据；

d）在CII废弃时，对其存储的数据及时处理。

13.5 供应链保障

CII运营者在供应链安全保障方面包括：

a）针对重要零部件，建立多级库存联动+安全库存多重保障，保持必要的供应弹性储备并自动补货；

b）建立供货商审核制度，及时淘汰、更新供货商名单；

c）制定设备、设施、系统等可替换方案，确保不少于2家以上独立供货渠道；

d）优先采购通过国家检测认证的设备和产品。

14 演练与培训

14.1 演练

CII运营者在应急演练方面：

a）制定年度网络安全应急演练计划，每年对应急预案至少演练一次；

b）按要求参加由国家网信部门、保护工作部门和公安机关等组织的跨组织、跨地域的网络安全应急演练；

c）围绕CII保护特点实施重点演练，如保障关键业务安全稳定运行，同一CII不同运营者之间、关键业务链上下游运营者之间的协同联动等。

14.2 培训

CII运营者在宣传培训方面：

a）针对网络安全应急预案涉及的部门和人员制定年度培训计划，通过编发培训材料、举办培训班、开展工作研讨等方式，对与应急预案实施密切相关的管理人员和专业救援人员等组织开展应急预案培训；

b）制定考评制度，对参加培训的网络安全应急工作人员进行考评，通过后才能继续担任网络安全应急工作岗位；

c）每年对培训计划与培训内容进行评估并持续更新。

参 考 文 献

[1] GB/T 19001—2016 质量管理体系 要求

[2] GB/T 19004—2015 质量管理体系 业绩改进指南

[3] GB/T 20984—2022 信息安全技术 信息安全风险评估方法

[4] GB/T 20985.1—2017 信息技术 安全技术 信息安全事件管理 第1部分：事件管理原理

[5] GB/T 20985.2—2020 信息技术 安全技术 信息安全事件管理 第2部分：事件响应规划和准备指南

[6] GB/T 22080—2016 信息技术 安全技术 信息安全管理体系要求

[7] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

[8] GB/T 31496—2015 信息技术 安全技术 信息安全管理体系实施指南

[9] GB/T 36466—2018 信息安全技术 工业控制系统风险评估实施指南

[10] GB/T 36635—2018 信息安全技术 网络安全监测基本要求与实施指南

[11] GB/T 38645—2020 信息安全技术 网络安全事件应急演练指南

[12] ISO/IEC 25024:2015 Systems and software engineering—Systems and software Quality Requirements and Evaluation (SQuaRE) —Measurement of data quality