ICS 35.020
L 80

团　　体　　标　　准

T/GDNS 004—2022

关键信息基础设施安全保障知识图谱管理模型和评价方法

Knowledge graph management model and evaluation method of critical information infrastructure security assurance

2022-03-28 发布　　2022-04-28 实施

广东省计算机信息网络安全协会　发布

目　　次

前　　言 II
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　关键信息基础设施安全知识图谱本体 2
5　关键信息基础设施信息安全保障评价方法 3
参考文献 4

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。

本文件由广东省计算机信息网络安全协会提出并归口管理。

本文件起草单位：广州绿盟网络安全技术有限公司、华南理工大学、广东省计算机信息网络安全协会、广州中医药大学、广东省清朗网络安全应急服务中心、广东省关键信息基础设施保护中心、广州大学。

本文件主要起草人：赖智全、陆以勤、缪婧、黄振毅、黄其森、肖岩军、陈嘉睿、沈雄、潘伟锵、温祥彬、罗杏娥、阮懿宗、覃健诚、程喆、王海瀚、毛中书、韩颖铮、谢婉娟、袁毅鸣、余骏华、梁倩、邓国强、唐玮俊、刘卫红、刘葵、郑媛、林茵、黎志生、艾飞、陈卓星、张洋、王猛、梁湘燕、黄建波、丁扬、钟培俊、唐文军、刘梅、潘周双、齐虹、王子仁、徐碧芸。

关键信息基础设施安全保障知识图谱管理模型和评价方法

1 范围

本文件规定了关键信息基础设施信息安全保障的知识图谱管理模型的基本概念，确立关键信息基础设施信息安全保障评价方法。

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千本文件；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—2010 信息安全技术 术语

GB/T 31495.1—2015 信息安全技术 信息安全保障指标体系及评价方法 第1部分：概念和模型

GB/T 31495.2—2015 信息安全技术 信息安全保障指标体系及评价方法 第2部分：指标体系

GB/T 31495.3—2015 信息安全技术 信息安全保障指标体系及评价方法 第3部分：实施指南

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

3 术语和定义

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

指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。

3.2

知识图谱 knowledge Graph

一种揭示实体之间关系的语义网络。

3.3

信息安全保障评价 evaluation of information security assurance

收集信息安全保障证据，并获得信息安全保障值的过程和途径。

3.4

信息安全保障能力 abilities of information security assurance

被保障实体安全防御、响应和恢复等特性的体现。

3.5

信息安全保障效果 effects of information security assurance

被保障实体的信息安全保障目标和属性的实现程度。

4 关键信息基础设施安全知识图谱本体

关键信息基础设施信息安全知识图谱本体采用过程方法建立的，本体包含了管理部分和技术部分，同时也包含了安全评估的三要素资产、脆弱性与威胁，是一个完善的关键信息基础设施安全知识图谱本体结构。

图 1 说明了关键信息基础设施安全保障知识图谱本体设计的详细信息，包括涉及的安全知识实体以及实体间的语义关系。其中国家关键信息基础设施政策文件为主要的实体类型，其对象是关键信息基础设施单位的网络安全情况，同时关键信息基础设施是基于《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》的三级或以上设立的，所以“关键信息基础设施政策”实体指导“关键信息基础设施检查要求”的制定和实施，其基本要求必然要覆盖包含等级保护的技术与管理要求。

关键信息基础设施信息安全知识图谱本体通过整合《关键信息基础设施安全保护条例》中相关的网络安全和数据安全要素及其关联特性，成为机器可读的执行检查标准，可以在关键信息基础设施相关规范新增或者等级保护要求内容更新时，自动更新对应的检测指标，以保证关键信息基础设施安全的实时性和有效性。

注：在不引起混淆的情况下，本文件中的《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》简化为“等级保护”。

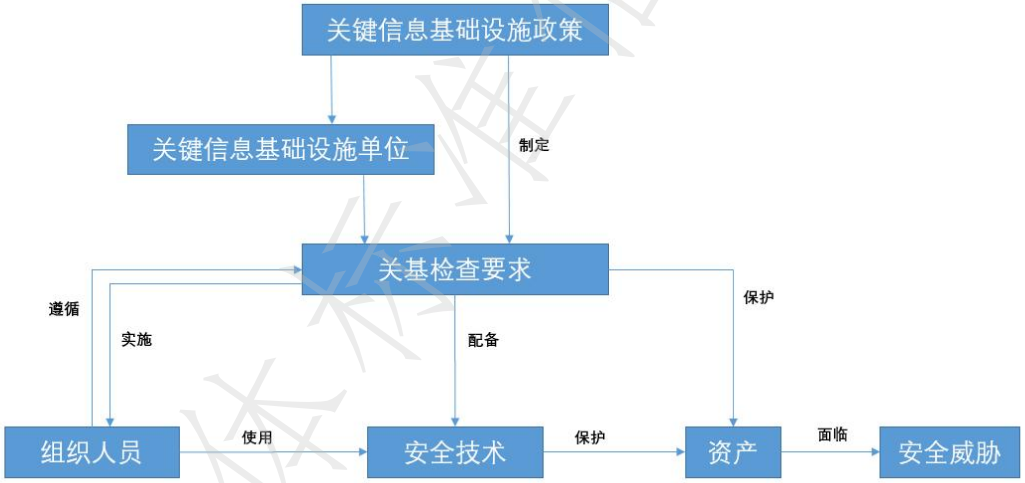

图 1 关键信息基础设施安全知识图谱本体

关键信息基础设施安全知识图谱实体类型说明

a) 关键信息基础设施政策：关键信息基础设施安全相关的政策、法规，指导关键信息基础设施的安全防护工作。

b) 关键信息基础设施单位：根据《中华人民共和国网络安全法》中规定归属于关键信息基础设施行业的实体单位。

c) 关键信息基础设施检查要求：依据关键信息基础设施安全相关的政策、法规进行指导制定的关键信息基础设施安全检查要求，具备可实操以及可量化的特性。

d) 组织人员：关键信息基础设施单位安全工作相关的责任人、执行者。

e) 安全技术：用于关键信息基础设施单位安全防护相关的信息技术。

f) 资产：归属于关键信息基础设施单位的相关实体/虚拟资产，包括但不限于：终端、服务器、软件、数据等。

g) 安全威胁：关键信息基础设施单位所遭受的不同类型的攻击。

知识图谱建立举例：

a) 关键信息基础设施政策——《GB/T 22239-2019 信息安全技术网络安全等级保护基本要求》或《关键信息基础设施安全保护条例》。
b) 关基检查要求——应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术实现。
c) 安全技术——密码技术；生物技术；多因子认证；数据安全防护技术，参考《中华人民共和国数据安全法》、《中华人民共和国密码法》和《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》。
d) 资产——单位人员终端账户。
e) 组织人员——关基单位工作人员。
f) 安全威胁——密码暴力破解。

5 关键信息基础设施信息安全保障评价方法

关键信息基础设施信息安全保障评价方法用于验证图1所示信息安全保障过程的有效性而开展的一系列评价活动。

图2说明了关键信息基础设施信息安全保障评价的过程，评价内容是基于关键信息基础设施的检查要求来设定的，一方面通过检查项的测量形成测量结果，另一方面是基于法规要求针对每个检查项形成安全的基线要求，最后通过测量结果与基线值的匹对，形成测量结果的汇总与评估，在测量结果的汇总中，会利用分析模型，检验关键信息基础设施检查要求的合理性并予以调整。

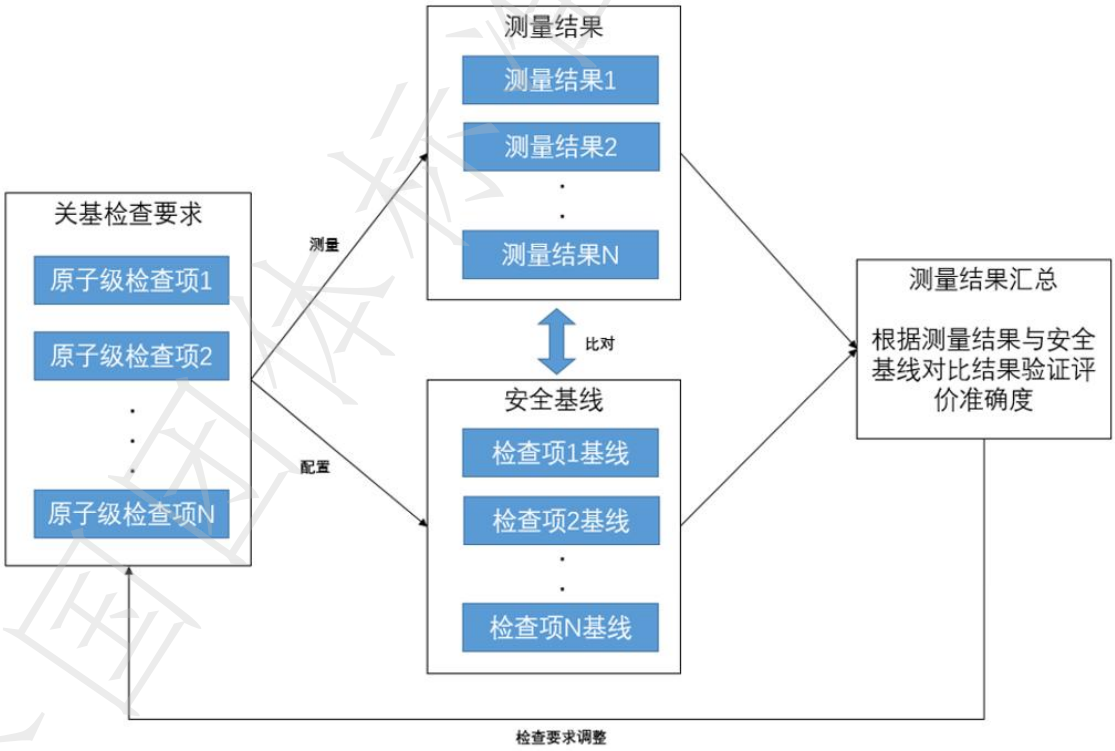

图2 信息安全保障评价方案

评价流程说明：
a) 将关键信息基础设施检查项要求拆分为原子级检查项。
b) 根据关键信息基础设施安全要求进行检查项基线配置。
c) 计算原子级检查项测量结果，比对安全基线。
d) 汇总测量结果并与关键信息基础设施单位实际情况比对验证，根据准确度对检查要求进行调整。

参 考 文 献

[1]中华人民共和国数据安全法（2021年6月10日第十三届全国人民代表大会常务委员会第二十九次会议通过）

[2]中华人民共和国个人信息保护法(2021年8月20日第十三届全国人大常委会第三十次会议通过)

[3]关键信息基础设施安全保护条例（2021年4月27日国务院第133次常务会议通过）

[4] ISO/IEC 15408-1:2009 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model

[5] ISO/IEC 27004:2009 Information technology –Security techniques – Information security management - Measurement

[6] NIST Special Publication 800-37: Guide for Applying the Risk Management

[7] Federal Information Security Management Act（联邦信息安全管理法案）

[8] National Security Agency. National Information Systems Security Glossary. NSTISSI 4009 Fort Meade, MD.Sept.2000.

[9] GB/T 22080-2008　信息安全管理体系 要求（ISO/IEC 27001:2005）

[10] GB/T 15443.1　信息技术 安全技术 信息安全保障框架 第1部分：综述和框架

[11] GB/T 19001-2008　质量管理体系：要求（ISO 9001:2008）

[12] GA/T 713-2007　信息安全技术 信息系统安全管理测评

[13] GB/T 22239-2008　信息安全技术 信息系统安全等级保护基本要求

[14] GB/T 18336-2001　信息技术 安全技术 信息技术安全性评估准则

[15] GB/T 18336.1-2008　信息技术 安全技术 信息技术安全性评估准则 第1部分：简介和一般模型

[16] 沈昌祥.信息安全工程导论[M].电子工业出版社，2003.7

[17] 吴世忠，陈晓桦，李鹤田，李斌等.信息安全测评认证－理论与实际[M].合肥：中国科学技术大学出版社，2006.

[18] 宁家骏.信息内容安全[M].贵州科技出版社，2004.5.