网络安全等级保护制度下的数据安全研究

李尚号，王　勇
（公安部网络安全等级保护评估中心，北京　100142）

摘　要：通过深度剖析网络安全和数据安全的内在联系，探讨将数据安全保护纳入网络安全等级保护工作流程的必要性与可行性，提出具体的工作步骤与实施过程。在落实等级保护的基础上，有序推进数据安全保护，快速、有效、体系化地开展数据安全保护工作，实现网络基础设施安全和上层业务数据安全一体的真正数据安全。

关键词：数据安全；网络安全等级保护；等级测评
中图分类号：TP393　　**文献标识码：**A　　**DOI：**10.19358/j.issn.2097－1788.2023.12.011
引用格式：李尚号，王勇. 网络安全等级保护制度下的数据安全研究［J］. 网络安全与数据治理，2023，42(12)：67－70，89.

Research of data security based on cybersecurity classified protection

Li Shanghao，Wang Yong
（MPS Cybersecurity Classified Protection Evaluation Center，Beijing 100142，China）

Abstract：This article explores the intrinsic connection between cybersecurity and data security and discusses the necessity and feasibility of incorporating data security protection into the cybersecurity classified protection. It proposes specific steps and implementation processes. Based on the implementation of cybersecurity classified protection，data security protection is systematically advanced in an orderly manner to achieve true data security that integrates network infrastructure security with upper-level business data security in a fast，effective，and systematic manner.

Key words：data security ；cybersecurity classified protection；evaluation for classified protection

0　引言

随着信息技术的广泛应用，网络空间逐步成为人类生产生活的重要场所，数据作为人类在网络空间中的行动痕迹，蕴含了丰富的信息。数据中所承载的价值对于国家稳定、社会秩序、个人利益具有重要影响。核心数据更是已成为各国的战略资产。根据《中国互联网络发展状况统计报告》显示，截至2023年6月，我国网民规模达10.79亿，互联网普及率达76.4%。我国人口基数大、互联网普及率高的基本国情势必会带来网民数据体量大、数据安全保护工作难度高等挑战。

2021年《数据安全法》和《个人信息保护法》相继颁布实施，代表着我国现行数据安全顶层法律法规日趋完善[1]，我国数据安全保护工作重心逐步从顶层立法向落地执行转移。《数据安全法》规定信息系统进行数据处理活动，首先要遵循网络安全等级保护制度，强调了网络安全与数据安全的关联关系和内在逻辑。

网络安全等级保护制度是中国目前体系最完整、技术最成熟、接受度和认可度最高、执行力度最强、覆盖范围最全面的国家网络安全基本制度体系，是《网络安全法》和《数据安全法》等国家网络安全多项法律明确要求施行的，为保护数据和个人信息安全做出了重要贡献。但是网络安全保护制度以系统为定级对象，更加注重系统整体的网络运行安全，对于数据的关注相对不足[2]。同时，等级保护中对于数据的保护偏向于传统的静态安全，未对于数据的全生命周期安全提出有效要求。面对新形势下数据安全发展的新要求、新挑战[3]，如何应用好网络安全等级保护制度对其进行全面保护是当前数据安全工作的重点。

1　网络安全等级保护与数据安全现状

在《网络安全法》颁布实施后，为了满足新形势下对网络安全的要求，网络安全等级保护相关标准也随之修订，形成了以《网络安全等级保护基本要求》（以下简称《基本要求》）[4]和《网络安全等级保护测评要求》（以下简称《测评要求》）[5]为核心的等保2.0标准体系。

《基本要求》对数据的完整性、保密性、备份恢复和个人信息保护等提出了具体要求，《测评要求》则规定了相关数据保护有效性的检验手段。

通过近几年的实施，等保 2.0 标准体系在我国网络安全和数据安全保护工作中发挥了巨大作用[6-7]，但是随着数据安全保护工作的深入，《基本要求》中的相关内容已无法满足数据采集、传输、存储、处理、交换和销毁全生命周期的安全要求，迫切需要建立一套完整的数据安全保护方案。

为落实《网络安全法》《数据安全法》和《个人信息保护法》中对数据安全的保护要求，延续并完善网络安全等级保护制度，公安行标《网络安全等级保护数据安全基本要求》《网络安全等级保护数据安全测评要求》相继立项，按照数据全生命周期规划四个等级的安全保护要求和测评要求。等级保护数据安全系列标准相互配合，对构建等级保护数据安全测评体系、掌握我国数据安全状况和防护水平、促进国家数据安全保障能力全面提升，具有重大意义。

2 数据安全保护工作流程分析

《网络安全法》从系统运行安全、网络信息安全角度提出了数据管理要求，管理对象侧重个人信息和关键信息基础设施收集产生的数据，管理范围侧重数据采集、存储等环节。《数据安全法》在此基础上作了进一步扩充，将任何以电子或其他方式记录的信息，全方面、全流程地纳入数据安全保护范畴。因此《数据安全法》是对《网络安全法》的补充和延续，是网络安全保护工作的继承和发展。

据统计，网络安全事件中大约有 70% 的比例是为了获取或者破坏其中的数据。网络安全的最终目的是保护数据安全，数据安全依赖于维护网络安全，数据安全与网络安全是一体两面、不可分割的，因此网络安全保护工作和数据安全保护工作具有深度耦合的基础。

通过上述分析不难看出，数据安全保护工作并不是独立存在的，而是应该与网络安全等级保护工作紧密结合、同步开展。网络安全等级保护工作包括定级、备案、安全建设整改、等级测评和安全检查五个主要环节[8]，与此对应数据安全保护工作也应当按照定级、备案、安全建设整改、数据安全测评、安全检查五个阶段开展工作。如此不仅可以充分发挥网络安全等级保护制度的经验优势，快速推进数据安全保护工作，还能够最大程度地减轻企业合规工作压力，进而促进等级保护工作的良性循环。

3 数据安全保护工作具体实施

为确保等级保护工作与数据安全保护工作能够紧密结合、同步开展，本文将按照数据安全定级、数据安全备案、安全建设整改、数据安全测评、安全检查五个关键动作，分析数据安全保护工作与等级保护工作同步实行的必要性与可行性，并提出具体实施方法。

3.1 数据安全定级

数据的收集、处理、存储都依赖于所属的信息系统，因此数据定级工作应当随信息系统定级同步开展。与等级保护系统定级类似，确定数据等级时应考虑数据泄露、破坏对公民、法人和其他组织的合法权益，社会秩序、公共利益，国家安全造成的侵害程度，并将信息系统的数据级别作为信息系统保护等级确定的考虑因素。

不同于网络安全系统等级的五个等级，数据按照其重要程度和影响程度，可分为核心数据、重要数据、一般数据三个等级。不同保护等级的信息系统能够承载的数据级别不同，具体对照如表 1 所示。

3.2 数据安全备案

数据安全备案应当在等级保护备案制度、标准、流程的基础上扩充数据相关要求，完善目前现有的等级保护备案平台，不增加工作流程负担，只需增加数据基本信息、数据处理信息、数据安全情况的报送。通过数据安全备案使公安机关摸清定级系统的数据保护情况，掌握数据种类与量级。

表 1 数据级别与网络安全等级对照表

数据级别	网络安全保护等级	说明
核心数据	第四级	对领域、群体、区域具有较高覆盖度或达到较高精度、较大规模、一定深度的重要数据，一旦被非法使用或共享，可能直接影响政治安全
重要数据	第四级、第三级	特定领域、特定群体、特定区域或达到一定精度和规模的数据，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全
一般数据	第四级、第三级、第二级、第一级	除核心数据和重要数据以外的其他所有数据，包括敏感一般数据和普通一般数据

数据安全责任单位依据相关标准规范开展数据识别工作，识别运营范围内的数据类别、级别和相关内容，识别数据后邀请外部专家进行评审，确定最终数据识别结果。数据识别完成后，数据安全责任单位通过等级保护备案平台向公安机关申报备案，提交备案材料等待公安机关审核，需要备案的数据信息至少应包括表 2 中的内容。

表 2　数据备案信息

数据备案信息	具体内容
数据基本信息	数据责任主体信息、安全负责人信息、所存储的数据量级、类别、范围、分类分级结果、承载数据的信息系统
数据处理信息	数据处理的目的与方式、处理规模、存储位置、存储期限、数据使用与共享的相关方信息、数据销毁原则
数据安全情况	数据安全管理制度、安全保护措施、数据安全评估结果、数据出入境安全评估结果和等级保护测评情况

公安机关应对数据信息和安全情况进行审核，通过审核的应当将备案结果与信息系统等级保护备案结果关联。

3.3　安全建设整改

网络系统在规划、建设阶段应充分考虑数据安全保护需求，在等级保护的基础上，结合数据全生命周期不同阶段的保护需求，设计数据安全保护方案，形成数据安全保护策略，构建数据安全保护体系。

数据安全责任单位应依据评估、检查发现的安全问题及风险进行数据安全建设整改工作，根据数据安全相关标准规范，结合安全问题及实际情况，对相关风险点进行整改。整改完成后应对整改结果进行自评估，并将安全问题列表、整改方案及实施情况、整改结果和整改后残余风险的处置情况等报送给公安机关。

3.4　数据安全测评

依托成熟完善的等级保护测评体系，在原有等级保护工作的基础上增加数据安全测评内容，开展数据安全测评工作。数据安全测评工作包括调研、方案编制、现场测评、分析与报告编制四个阶段，四个阶段工作可与等级保护测评同步展开，也可根据需求开展单独的数据安全测评。具体工作内容和流程如图 1 所示。

（1）调研阶段

在进行等级测评工作的同时，测评机构依据相关标准规范对数据安全开展测评，通过查阅相关资料、填写数据调研表格、现场沟通调研等方式对信息系统的数据基本情况进行调研，形成数据资产调研表，调研表中应包括以下内容：

数据基础信息：数据所属单位信息、数据责任方信息、安全负责人信息。

数据基本信息：数据分类分级结果、量级、类型、范围、存储位置及期限、重要程度。

相关数据资产：相关设备、数据应用、管理软件等信息。

数据处理情况：数据处理、流动、共享、销毁等相关情况。

（2）方案编制阶段

测评机构根据数据基本情况的调研结果，分析承载数据对象信息系统的业务流程，明确数据活动涉及的资产，确定本次测评的数据对象范围，最终形成数据安全测评方案，方案中应对项目背景、测评对象、选用指标、测评方法、风险规避措施、工作计划等进行详细说明。

（3）现场测评阶段

测评机构依据相关标准规范和测评方案抽选的测评指标对信息系统数据的采集、存储、处理、传输、交换、销毁等活动开展测评，通过现场访谈和核查、结合工具检查的方式测评数据全生命周期活动中是否存在合规风险、安全风险，安全测评内容包括但不限于以下：

数据活动合规性：数据收集、存储、处理、传输、交换、销毁等活动是否符合相关法律法规要求，是否存在过度收集、数据滥用、跨境共享等相关行为。

数据管理活动：核查组织架构和数据管理人员配置的合理性，数据安全管理制度的完备性，数据安全管理流程的完整性，个人信息保护管理制度及措施的有效性等。

数据技术措施：数据的保密性、完整性、真实性相关保护措施是否有效，访问控制及认证措施强度、密码技术应用是否合理，数据活动的审计是否覆盖全面，数据资产识别是否准确完备等。

（4）分析与报告编制阶段

测评机构依据相关标准规范和现场测评结果对信息系统现有的数据安全措施进行分析，分析存在的安全风险并提出整改建议，得出数据安全测评结论，形成数据安全测评报告。

3.5　安全检查

公安机关依法开展监督检查工作，依据国家相关法规对信息系统数据进行分类、分级合规性检查，审查这些重要数据在采集、存储、传输或使用上的安全性和合规性。对信息系统中的各类网络安全威胁、信息系统脆弱漏洞环节等方面进行检测，评估出业务信息系统的数据风险点和风险阈值，控制信息数据安全风险，消除数据安全隐患，实现数据安全的可知、可管、可控。

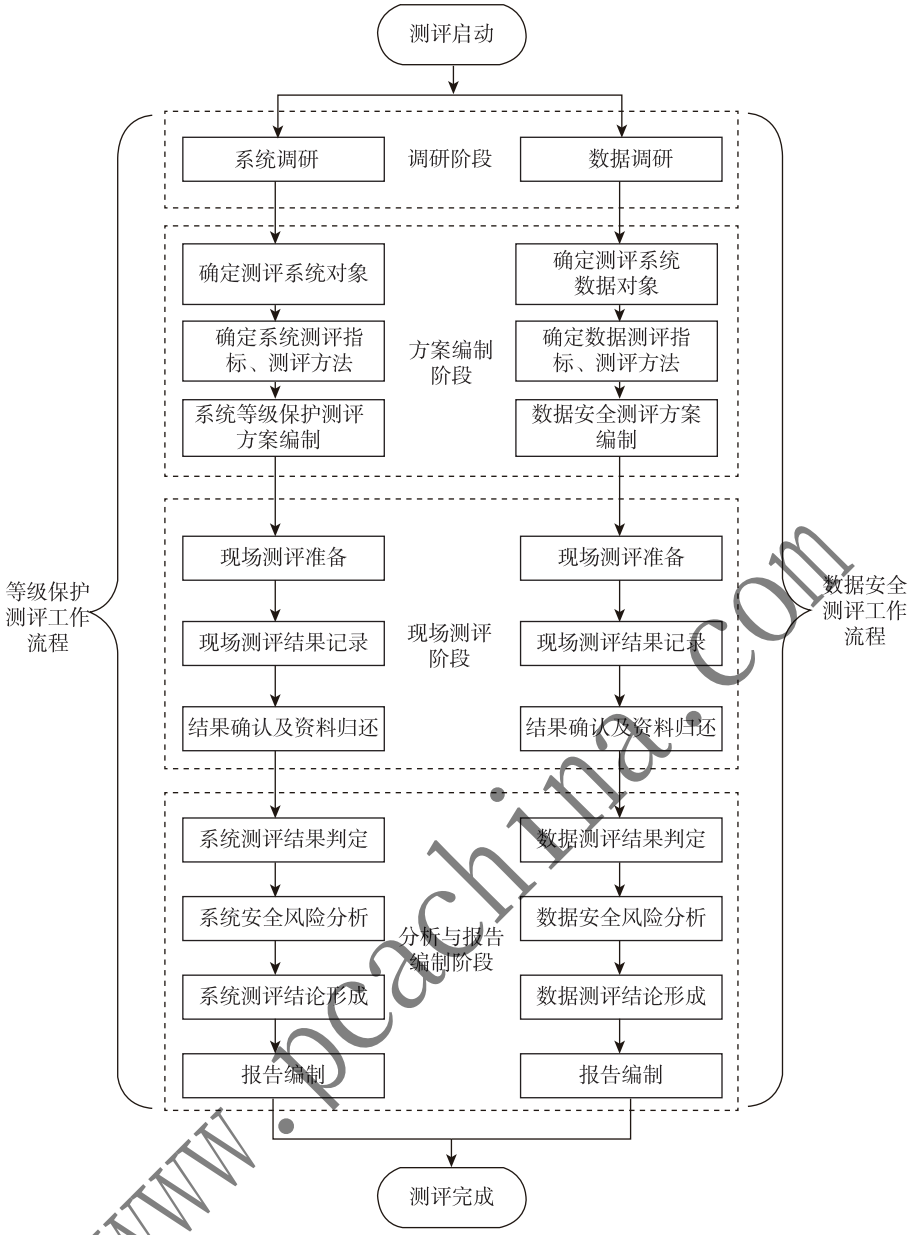

图 1　等级保护测评与数据安全测评工作流程

4　结论

网络基础环境承载数据和个人信息，数据和个人信息依托网络基础环境，维护网络安全的目的是保护数据和个人信息安全，保护数据和个人信息安全有赖于维护网络安全。网络安全与数据安全相互依存、密不可分，数据安全保护工作与网络安全等级保护工作同步开展具有内在逻辑与工作基础，而脱离基础环境和信息系统的数据安全保护工作将缺乏底层支撑与有力抓手。因此当前形势下，将数据安全纳入网络安全等级保护制度是快速推进我国数据安全建设的有效手段。

参考文献

[1] 洪延青. 我国数据安全法的体系逻辑与实施优化 [J]. 法学杂志，2023，44（2）：38－53.

[2] 刘爱娇，孙越洋. 深化公安改革促进网络安全等级保护工作的思考 [J]. 网络安全技术与应用，2021（5）：149－152.

[3] 王玉，安鹏，栗文科，等. 政务数据安全治理体系研究与实践 [J]. 信息安全研究，2023，9（9）：900－907.

[4] 马力，祝国邦，陆磊. 《网络安全等级保护基本要求》（GB/T 22239－2019）标准解读 [J]. 信息网络安全，2019（2）：77－84.

（下转第 89 页）

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部