面向电信行业的数据安全有效性验证方法论研究

张　侃[1]，刘坚桥[2]，刘孝颂[3]

（1. 中国电信股份有限公司，北京　100031；2. 中国电信股份有限公司江西分公司，江西　南昌　330029；
3. 中国电信股份有限公司研究院，上海　200120）

摘　要：在数字经济蓬勃发展的趋势下，数据资产已成为电信运营商的核心竞争力载体。如何统筹好数据合规运营和风险防范是摆在电信运营商面前的必答题。针对当前数据安全领域缺乏系统性的有效性验证方法论来评价企业在合规满足、安全防护、事件响应等方面的综合水平，构建了一个面向电信行业的“数据安全有效性验证体系”，并结合实践经验，提出了包含“合规域、技术域、事件域”的三域一体验证框架。该框架建立了一套从“满足合规”到“实战有效”的评价机制，为电信运营商行业乃至其他数据运营者的数据安全治理提供了一种新思路。

关键词：数据安全；有效性验证；电信行业；安全合规

中图分类号：TP309　　**文献标志码：**A　　DOI：10. 19358/j. issn. 2097-1788. 2026. 07. 004

中文引用格式：张侃，刘坚桥，刘孝颂. 面向电信行业的数据安全有效性验证方法论研究[J]. 网络安全与数据治理，2026，45(7)：24-31.

英文引用格式：Zhang Kan，Liu Jianqiao，Liu Xiaosong. Research on data security effectiveness verification methodology for the telecommunications industry[J]. Cyber Security and Data Governance，2026，45(7)：24-31.

Research on data security effectiveness verification methodology for the telecommunications industry

Zhang Kan[1]，Liu Jianqiao[2]，Liu Xiaosong[3]

（1. China Telecom Corporation Limited，Beijing 100031，China；2. Jiangxi Branch of China Telecom Corporation Limited，Nanchang 330029，China；3. Research Institute of China Telecom Corporation Limited，Shanghai 200120，China）

Abstract：Under the trend of booming digital economy，data assets have become the core competitiveness carrier for telecommunications operators. How to coordinate data compliance operations with risk prevention constitutes an imperative challenge confronting the industry. Currently，there lacks a systematic methodology for effectiveness validation to comprehensively evaluate enterprises′ capabilities in compliance fulfillment，security protection，and incident response within the data security domain. This study aims to establish a "Data Security Effectiveness Verification System" tailored for telecommunications industry，proposing a tri-domain verification framework encompassing compliance，technical，and incident dimensions based on China Telecom′s practical experience. The framework develops an evaluation mechanism progressing from "compliance achievement" to "operational efficacy"，providing a novel approach for data security governance among telecom operators and other data-driven entities.

Key words：data security；effectiveness validation；telecommunications industry；security compliance

0　引言

在数字经济浪潮下，数据已成为与土地、劳动力、资本、技术并列的新型生产要素[1]。随着数据要素市场建设的不断推进，电信运营商作为数据密集型企业的数据合规问题日益凸显[2]。电信运营商业务系统承载着用户身份信息、通信数据、位置信令、消费行为等敏感数据，这些数据的体量巨大、类型多样、价值密度高、流动性强，被不法分子视为“金矿”。近年来，全球范围内针对电信运营商的数据安全事件频发，如2021年T-Mobile超过5 000万用户数据被窃取事件[3]为全行业敲响了警钟。

面对严峻的安全形势和日益收紧的全球数据保护

法规[4-5]，电信运营商在数据安全领域持续加大投入，不断完善管理体系和各类防护技术。然而，如何科学评估这些安全投入的真实成效以及体系在真实攻击下的韧性，成为普遍痛点，突显了从“合规建设”到“实战有效”的鸿沟。相较于网络安全有效性验证的成熟技术体系，如渗透测试（Penetration Testing）、攻击与入侵模拟（Breach and Attack Simulation，BAS），数据安全有效性验证仍处于探索阶段，缺乏系统性的方法论指导。

本研究聚焦于构建一套系统性、科学化的方法论，用以度量和验证电信行业数据安全防护体系的真实有效性，旨在提出一个融合“合规性、技术性、事件响应”三个维度的数据安全有效性验证框架，并基于实践案例进行分析，以验证其可行性与应用价值。

1 相关工作

1.1 网络安全有效性验证技术评述

网络安全有效性验证的核心目标在于评估安全控制措施在真实威胁环境中的防护效能。例如，漏洞扫描（Vulnerability Scanning）聚焦于识别已知漏洞，渗透测试则通过模拟攻击者行为探测系统弱点。随着攻防对抗升级，红蓝对抗演练与 BAS 技术逐渐兴起，BAS 平台可自动化、持续性地模拟多样化攻击战术、技术与过程（Tactics，Techniques and Procedures，TTPs），量化评估安全产品（如防火墙、终端检测响应系统）的检测拦截效率，并为安全运营提供持续性反馈[6]。在评估安全运营能力时，平均检测时间（Mean Time to Detect，MTTD）和平均响应时间（Mean Time to Respond，MTTR）是两个关键量化指标[7]。尽管这些技术在网络边界与终端防护验证中成效显著，其局限性亦日益显现：它们主要集中于基础设施及系统脆弱性评估，对数据本体安全状态、复杂业务逻辑风险以及合规性要求的验证能力存在显著不足。

1.2 数据安全验证的独特性与挑战

数据安全有效性验证与网络安全验证存在较大差异，其独特性和挑战主要体现在以下三个方面：

（1）合规性约束的复杂性：数据安全的核心驱动力源于法律法规遵从。验证工作需双重聚焦：既评估技术防护效能，同时需确保数据处理全流程符合法定要求（如告知同意原则、数据最小化原则、主体权利保障等），这使得验证目标与评价体系呈现显著多元性。

（2）数据本体的全生命周期覆盖：验证焦点必须由承载系统转向数据本体本身，贯穿采集、传输、存储、处理、共享至销毁的全生命周期。典型验证任务包括数据分级分类准确性校验、加密措施跨场景有效性验证、脱敏数据再识别风险评估等。已有学者对数据安全实践进行了系统性综述，并探讨了机器学习带来的新挑战[8]。但总体来说，这一领域的验证方法论研究尚处于起步阶段。

（3）结果导向与影响评估：数据安全事件的实际后果（如数据泄露、篡改、服务中断）构成终极验证标准。方法设计需超越单纯攻击拦截检测，重点评估事件发生时业务连续性保障能力及对客户信任、企业声誉的影响可控性，内嵌业务影响分析成为必要维度。此外，零信任架构所倡导的“持续验证、永不信任”理念也为数据安全验证提供了新的思考方向[9]。

1.3 现有数据安全框架与本研究的关系

国际上已存在多个广受认可的安全框架，如 NIST 网络安全框架（Cybersecurity Framework，CSF）、ISO/IEC 27001/27701 系列标准等。这些框架为组织建立信息安全和隐私保护管理体系提供了全面的控制项清单，回答了“需要做什么”的问题。然而，它们并未提供一套系统性的方法来验证这些控制项“做得怎么样”，即其部署的有效性如何。尽管有学者尝试基于 NIST CSF 构建网络安全成熟度评估框架，但其输出结果仍偏向于定性描述，缺乏量化验证机制[10]。

在数据安全验证的具体实践中，一些组织和机构也提出了相关的指导建议或评估模型，但均存在一定的局限性，难以直接应用于电信行业的综合性验证。云安全联盟（CSA）发布的《云数据安全指南》及相关的验证建议侧重于云环境下的数据安全控制，其验证思路主要围绕控制措施的“存在性”检查，缺乏对控制措施“有效性”的动态、量化评估手段。例如，CSA 建议检查加密配置是否启用，但并未提供如何验证加密算法强度、密钥管理安全性的具体攻击模拟方法。开放 Web 应用程序安全项目（OWASP）提出的数据安全验证清单主要聚焦于应用层的数据安全风险，如 SQL 注入导致的数据库泄露、不安全的直接对象引用（IDOR）等。其验证视角局限于应用程序层面，未能覆盖电信运营商所面临的复杂基础设施安全、全生命周期数据本体安全以及组织级合规治理验证的综合性需求。此外，国际数据管理协会（DAMA）的数据管理知识体系（DMBOK）虽提及数据安全活动的度量，但停留在成熟度评估层面，未构建起可操作的、结合实战对抗的验证技术栈。

综上所述，现有框架和指南或侧重于单一领域，或聚焦于静态合规检查，缺乏一个将“合规治理、技术防护、实战响应”三者有机融合，并通过量化模型进行综合评价的闭环验证体系。与此同时，数据要素流通中的风险评估与防范[11]以及数据空间安全分析[12]等领域的研究也表明，业界对跨域、动态的验证需求日益迫切。本研究提出的数据安全有效性验证方法论，并非替代既有框架，而是为其提供关键的闭环验证机制。其核心价值在于聚焦安全治理中最薄弱的“验证”环节，通过构建可度量、可复现、可持续的评估体系，推动静态合规要求向动态安全能力的转化。

2 面向电信行业的数据安全有效性验证方法论

2.1 总体框架与设计思想

本研究提出的方法论以确保合规底线与防范实际风险为核心目标，构建了一个“三域一体”的综合验证框架。其核心设计思想在于实现从顶层治理到底层技术，再到实战对抗的层层递进与闭环验证。如图 1 所示，该框架由合规域（Compliance Domain）、技术域（Technical Domain）和事件域（Event Domain）三部分组成，三大验证域相互关联、互为补充，共同构成一个动态、持续的评估与优化循环，确保数据安全体系在理论、实现和实战三个层面均能实现既定目标。

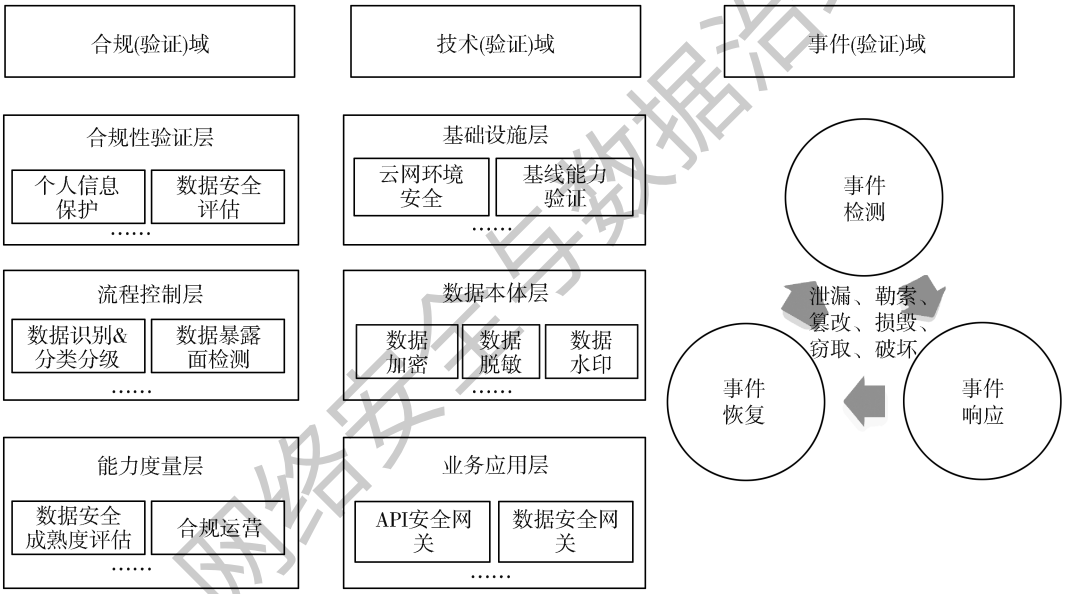

图 1　数据安全有效性三域一体验证框架

2.2 合规域验证：确保依法合规的治理底线

合规域验证的核心是检验组织的数据安全治理体系是否全面、有效地满足了内外部的合规要求。它分为三个层次：

（1）合规性验证层：聚焦于法律法规的刚性约束。验证内容重点围绕《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》以及行业标准（如 GB/T 35273－2020《信息安全技术 个人信息安全规范》[5]）的核心条款，如数据出境安全评估、个人信息处理的“告知-同意”机制、敏感个人信息的特殊保护要求等。验证手段主要采用数据安全合规审计和数据保护影响评估（Data Protection Impact Assessment，DPIA），将法律条文转化为可检查的验证项，逐一核实其在业务系统和管理流程中的落地情况。

（2）流程控制层：关注管理制度和流程的执行有效性。该层核心是验证数据分类分级的准确性与一致性、数据资产清单的全面性以及数据处理活动记录的完整性。验证手段通常采用自动化数据发现与数据暴露面检测工具，识别未被纳管的“影子数据”和不合规的数据共享接口，从而检验管理流程是否存在执行偏差或覆盖盲区。

（3）能力度量层：旨在评估组织整体的数据安全能力成熟度。验证手段是引入业界通用的数据安全成熟度模型（Data Security Maturity Model，DSMM）进行评估。通过对组织架构、制度流程、技术工具、人员能力等多个维度进行量化打分，系统性地定位能力短板，为后续的安全建设投资和能力提升规划提供数据支撑。

2.3 技术域验证：构筑纵深防御的技术基石

技术域验证的核心是检验用于保护数据的各项技

术控制措施是否正确部署、合理配置并有效运行。它同样分为三个层次：

（1）基础设施层：电信行业广泛应用云平台、大数据平台和5G核心网等复杂基础设施，其自身的安全性是数据安全的基础。验证手段包括执行云安全配置管理（Cloud Security Posture Management，CSPM）进行基线核查，确保计算、存储、网络资源配置符合安全最佳实践；以及定期的主机与网络设备漏洞扫描，验证访问控制策略、网络隔离措施的有效性，特别是针对5G网络虚拟化和业务化架构带来的新风险点，例如有研究探讨了在5G VNF安全监控中利用联邦学习平衡隐私保护与安全监测效能的方案[13]。

（2）数据本体层：此层面关注直接作用于数据本身的安全技术。验证手段包括但不限于：

①数据加密验证：抽查验证敏感数据在传输（in-transit）和存储（at-rest）状态下是否均采用高强度加密算法，并对密钥管理生命周期的安全性进行审计。

②数据脱敏验证：在开发、测试、分析等场景下，兼顾数据可用性的同时评估数据脱敏的效果，重点采用k-匿名模型进行重识别评估，以检验脱敏后的数据是否存在再识别风险。对于脱敏后的数据集，计算数据集的k值（即任何一条记录在数据集中至少与$k-1$条其他记录在准标识符属性上不可区分）。通过计算准标识符列（如年龄、身份证、手机号等）的组合，评估其k值是否达到预设的安全阈值（例如$k\geqslant5$）。

③数据水印验证：通过受控的模拟数据泄露场景，验证数字水印技术在数据溯源中的有效性，包括水印的嵌入鲁棒性、提取准确性和溯源定位能力。以鲁棒性为例，可引入基于生成对抗网络（GAN）的水印去除攻击模拟。搭建一个包含生成器和判别器的GAN网络，生成器学习带水印数据的分布并尝试生成去除水印后的“干净”数据，判别器则试图区分生成的数据与原始无水印数据。通过在GAN训练过程中评估水印检测率的变化，可量化水印算法在面对基于深度学习的智能去除攻击时的鲁棒性。

（3）业务应用层：此层面关注通过业务系统访问和处理数据时的安全性和连续性。验证手段包括但不限于：

①API安全测试：对提供数据服务的API接口进行严格的安全测试，验证其在认证、授权、访问频率、输入参数等方面的控制是否有效，防止数据通过API泄露或被滥用。

②业务连续性验证：开展定期的数据灾备切换演练，真实检验恢复时间目标（Recovery Time Objective，RTO）和恢复点目标（Recovery Point Objective，RPO）的达成率；进行数据备份恢复测试，确保备份数据的完整性和可用性。

2.4 事件域验证：检验实战对抗的响应能力

事件域验证的核心是在模拟真实攻击场景下，检验安全体系的监测、响应和恢复的综合能力。它是一个完整的闭环流程：

（1）场景设计与攻击执行。第一步需要设计贴近电信行业特点的高频威胁场景，例如内部员工利用权限窃取核心客户资料、外部黑客利用Web应用漏洞进行“拖库”、勒索软件加密核心计费数据库等。第二步则利用自动化攻击模拟平台（BAS）或专业的人工红队，在可控范围内按照设计好的场景实施模拟攻击。

（2）能力验证与度量。在攻击过程中及之后，对以下关键能力进行度量：

①检测能力（Detect）：度量从攻击行为发生到被安全监测系统（如SIEM、UEBA）首次有效告警的平均时间，即平均检测时间（MTTD）。同时评估告警的准确率和误报率。

②响应能力（Respond）：度量从有效告警生成到安全团队完成初步遏制（如隔离受感染主机、封禁恶意IP、阻断数据外传通道）的平均响应时间（MTTR）。

③恢复能力（Recover）：在模拟攻击造成数据损坏或系统宕机后，验证IT和业务团队能否在预设的RTO/RPO目标内，利用备份和灾备机制恢复业务系统和数据，并对潜在的客户影响进行评估。该项能力同步反应了应急响应预案的可操作性。

2.5 有效性验证结果度量

基于以上有效性评估框架，可构建有效性验证结果度量体系：

$$\mathrm{Risk}=\alpha\cdot\sum_{i=1}^{n}\frac{|C_{\mathrm{req}_i}-C_{\mathrm{act}_i}|}{C_{\mathrm{req}_i}}+\beta\cdot\prod_{j=1}^{m}(1-E_{\mathrm{tech}_j})+\gamma\cdot\int_{t_0}^{t_1}I(t)\,\mathrm{d}t \tag{1}$$

其中，Risk为数据安全能力体系失效风险（0为最佳），α为合规权重，β为技术权重，γ为事件权重，$\alpha+\beta+\gamma=1$，且$\alpha,\beta,\gamma\in[0,1]$。其他参数说明见表1。

表 1　数据安全有效性验证的参数定义

参数	物理意义	验证域关联
C_{req}/C_{act}	合规要求值与实际值的偏差度，反映政策落地差距（如加密强度未达《数据安全法》要求）	合规域：通过自动化策略引擎实时比对法律条款与技术配置，量化合规缺口（示例：检测到 32% 存储未满足加密要求）
E_{tech}	技术防护有效性系数（0~1），如加密算法破解概率、脱敏数据可还原率	技术域：通过混沌工程模拟攻击，测试技术失效场景（示例：AES-256 加密有效性 $E_{tech}=0.999$）
$I(t)$	事件影响随时间衰减函数，体现响应延迟导致的损失放大效应	事件域：基于 MTTD 和 MTTR 计算累积损失（示例：勒索软件攻击 $I(t)=e^{-0.1t}$）

2.5.1　模型参数的确定依据

（1）权重确定方法。模型中合规域权重 α、技术域权重 β 与事件域权重 γ 的确定主要基于电信行业数据安全治理的实践特征，结合层次分析法（AHP）与专家德尔菲法综合得出。本研究组织了由 15 名行业专家（包括电信运营商安全主管 5 名、数据安全合规法律专家 4 名、网络安全厂商技术专家 6 名）组成的评估小组。评估过程如下：

首先，构建三域之间的相对重要性比较矩阵。专家一致认为，在数据安全领域，“事件域”的实战响应能力直接反映了安全体系的最终表现，其重要性最高；而“合规域”是法律底线，“技术域”是支撑手段，二者重要性相当。基于此，通过 AHP 计算得到一致性比例 CR<0.1，通过一致性检验。最终归一化权重向量为：$\alpha\approx0.3$，$\beta\approx0.3$，$\gamma\approx0.4$。本文后续实验即采用此基准权重。

（2）$I(t)$ 函数的具体形式与参数标定。风险公式中的积分项 $\int_{t_0}^{t_1} I(t)\,dt$ 用于量化事件发生后的累积损失。根据数据安全事件响应领域的研究，事件影响随时间通常呈现先指数增长后趋于平缓的指数衰减模型。其具体形式为：

$$I(t)=I_0\cdot e^{\{-\lambda(t-t\_detect)\}} \tag{2}$$

其中 $t\geqslant t\_detect$；I_0 为初始影响系数，由事件类型和受损数据量决定。在本文案例中，根据数据级别 I_0 设定为 0.8。t_detect 为攻击被检测到的时刻（即 MTTD）；λ 为衰减速率参数，反映响应效率。λ 与 MTTR 成反比，可通过历史事件数据进行回归标定。本文根据电信行业应急演练经验数据，标定 $\lambda=\ln(2)/MTTR\_baseline$，其中 MTTR_baseline 为基线平均响应时间（如 30 min）。对于事件管理过程的量化评估，已有学者提出了如 BenchIMP 等基准测试方法，为参数标定提供了参考思路[14]。类似的风险评估方法论也在 ICT 系统安全认证领域得到应用[15]，而形式化验证框架在 NDN 访问控制[16]等场景的成功实践也证明了量化评估的可行性。

2.5.2　模型参数的敏感性分析

为评估权重设定的微小变化对最终风险值的影响，本文进行了单因素敏感性分析。将案例中 γ 的取值在 0.3 至 0.5 区间内以 0.05 为步长逐次变动，同时按比例调整 α 与 β 以确保三者之和恒为 1。结果表明，当 γ 从 0.3 增至 0.5 时，系统失效风险值 Risk 在［0.312，0.398］区间内波动，变化幅度约为 24%。尽管风险绝对值存在一定变动，但该范围始终落于“风险较高、需立即整改”的定性判定区间内，未改变对系统风险等级的结论，从而验证了模型评价结果的鲁棒性。该敏感性分析框架亦可作为企业根据自身业务容忍度动态调整权重配比的量化参考工具。

3　体系应用与有效性评测

3.1　案例背景：电信运营商某测试业务系统

实验选取了电信运营商某测试业务系统作为评测对象，该系统处理用户资费、通信行为、地理相关的 A、B、C 三类信息，部署于混合云环境。该系统面临来自外部黑客攻击、内部数据滥用、第三方应用数据泄露等多重风险，是数据安全防护的重要对象。

依据本文提出的数据安全有效性验证框架，对该系统进行了一轮全面的有效性验证。结合该系统的业务特点，设 $\alpha=0.3$，$\beta=0.3$，$\gamma=0.4$，以下为部分有效性验证实施用例。

3.2　有效性验证实施过程

3.2.1　合规域验证

（1）实施：对照《个人信息保护法》和 GB/T 35273 标准，对 APP 的隐私政策、数据采集、数据提供构建测试用例（如表 2 所示），利用静态代码分析工具扫描 APP 安装包，验证其权限申请是否遵循“最小必要”原则。

（2）评估：对照测试用例对 APP 的隐私政策、数据采集、数据提供三方面内容进行验证，结果显示，9 项检查项中有 2 项未通过，不合规率为 22.2%。其中未通过项分别为在隐私政策方面，没有逐一列出第三方收集使用个人信息的目的、方式、范围等；在数据采集阶段，首次启动时申请了非必要的“读取通讯录”权限。

表 2　合规域评估用例

类别	合规要求
隐私政策	明示收集、使用个人信息的业务功能，以及各业务功能分别收集的个人信息类型。涉及个人敏感信息的，需明确标识或突出显示
	明示收集使用个人信息的目的、方式和范围： （1）逐一列出 APP 收集使用个人信息的目的、方式、范围等； （2）逐一列出第三方收集使用个人信息的目的、方式、范围等
	公开收集使用个人信息的规则： （1）隐私政策通过弹窗、文本链接、附件、常见问题等界面或形式展示； （2）提示用户阅读隐私政策等收集使用规则； （3）隐私政策等收集使用规则易于阅读； （4）向用户提供 APP 产品隐私政策摘要
	内容发生变化时，应及时更新个人信息保护政策并重新告知个人信息主体
数据采集	采用合法的方式收集个人信息，不应隐瞒产品或服务收集个人信息的功能
	遵循必要原则，仅收集与其提供的服务直接相关的个人信息： （1）不得收集与业务功能无关的个人信息； （2）用户可拒绝收集非必要信息或打开非必要权限； （3）收集个人信息的频度不得超出业务功能实际需要
	征得用户同意后才收集个人信息： （1）不得以默认选择同意隐私政策等非明示方式征求用户同意； （2）收集个人信息或打开可收集个人信息权限前征得用户同意； （3）同步告知申请打开权限和要求提供个人敏感信息的目的； （4）使用扩展业务功能时单独征得用户同意
数据提供	经用户同意后才向他人提供个人信息： （1）向他人提供个人信息前征得用户同意； （2）向接入的第三方应用提供个人信息前经用户同意； （3）明确共享、转让、公开披露个人信息无需征得同意情况
	提供个人信息前，开展个人信息安全影响评估

3.2.2　技术域验证

（1）实施：对存储用户身份信息的数据库进行加密有效性测试，确认加密算法符合国家标准；对提供用户账单查询功能的 API 进行脱敏能力验证；对数据库网关针对敏感操作的识别与拦截能力进行验证。构建技术域测试用例如表 3 所示。

（2）结论：存储用户身份信息的数据库采用国密算法实现有效加密。抽查的 100 条敏感个人信息中 90 条数据有效脱敏；数据库网关能有效记录所有查询操作，其中未经审批的 100 条高危操作均被拦截。整体技术防护失效率为 7.1%。技术域测试结果如表 4 所示。

表 3　技术域测试用例

类别	技术要求
数据水印	（1）对所有对外公开的敏感数据，强制嵌入不可见或可见的数据水印； （2）针对不同类型数据采用不同的水印技术； （3）通过 GANN 对抗检测水印鲁棒性； （4）定期检查水印的抗攻击性，确保其不易被去除或篡改
数据脱敏	（1）具备《数据脱密规范》，明确需要数据脱敏处理的应用场景、脱敏规则、脱敏方法、强度要求和使用限制等； （2）具备数据脱敏系统，强制执行敏感数据自动化脱敏处理； （3）重点采用 k-匿名模型进行重识别评估，以检验脱敏后的数据是否存在再识别风险； （4）定期评估脱敏效果，防止逆向工程
数据访问控制	（1）建立基于角色的访问控制，精细化权限； （2）遵循最小够用、职权分离等原则，授予用户权限； （3）定期审查更新权限，及时清理冗余权限； （4）定期进行账号权限开通和使用行为审计
传输加密	（1）涉及敏感数据的传输通道必须采用强加密协议和高强度加密算法； （2）确保加密证书安全，定期更新密钥； （3）在跨网络、跨地域传输敏感数据时，使用 VPN、专线等安全传输通道进行数据传输

表 4　技术域测试结果

类别	测试结果	是否符合要求
数据水印	（1）对外提供或公开敏感数据时，嵌入数据水印； （2）针对不同类型数据采用不同的水印技术； （3）定期检查水印的抗攻击性	符合要求
数据脱敏	（1）具备《数据脱密规范》，明确需要数据脱敏处理的应用场景、脱敏规则、脱敏方法、强度要求和使用限制等； （2）具备数据脱敏系统，敏感数据未全部脱敏，抽查的 100 条中 90 条数据有效脱敏； （3）脱敏算法符合要求； （4）定期评估脱敏效果，防止逆向工程	部分符合
数据访问控制	（1）建立基于角色的访问控制，精细化权限； （2）遵循最小够用原则，为用户授予权限； （3）定期审查更新权限，及时清除冗余权限； （4）定期进行账号权限开通和使用行为审计	符合要求
传输加密	（1）涉及敏感数据的传输通道采用 TLS 1.2 加密协议和国密 SM4 高强度加密算法； （2）定期更新密钥； （3）在跨网络、跨地域传输敏感数据时，使用 VPN、专线等安全传输通道进行数据传输	符合要求

3.2.3　事件域验证

（1）整体方案

依托数据安全 BAS 平台，模拟内部人员通过堡垒机批量导出敏感客户联系方式的行为。

（2）验证架构

验证架构如图 2 所示。

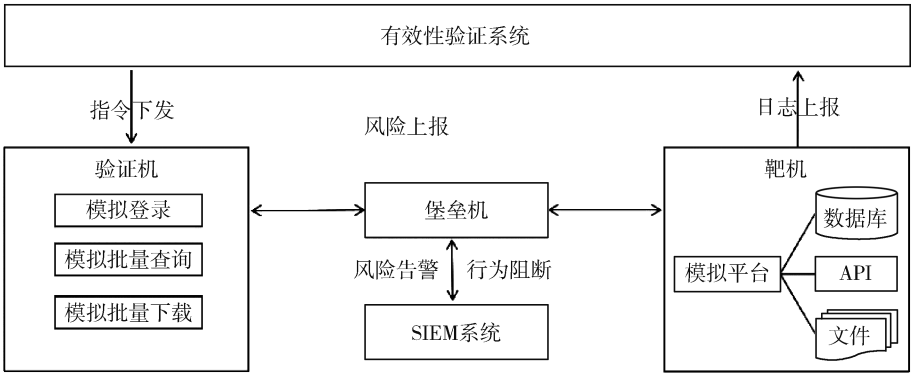

图 2　有效性验证实验场景示意图

（3）执行方案

阶段 1：攻击模拟。平台通过下发具体指令，制定详细的模拟验证行为方案，模拟内部运维人员使用合法凭证登录堡垒机系统，发起高频、大批量数据查询或导出操作，例如针对数据库执行重复性 SELECT 命令或导出 CSV 文件；同时，尝试通过压缩文件（如 ZIP 格式）或加密文件（如 AES 算法）等方式伪装数据，以绕过安全检测机制，测试系统防御的脆弱性。

阶段 2：检测。安全信息与事件管理（SIEM）系统实时监控日志数据，通过预设规则（如异常登录频率、数据流量阈值）检测到上述模拟操作中的异常行为特征，系统自动分析并产生高优先级告警，触发通知到安全运营中心。

阶段 3：响应。安全编排自动化与响应（SOAR）平台立即执行预定义剧本，剧本步骤包括验证告警真实性、确认攻击源后，自动阻断相关会话连接，并冻结涉事用户账号；同时，剧本触发事件记录和通知流程，确保团队及时介入处理。

阶段 4：影响评估。根据事件响应后的数据分析，评估潜在影响范围（如涉及敏感数据暴露风险），确定事件影响系数。根据 2. 5. 1 节定义的 $I(t)$ 函数进行量化，本次模拟中 $I_0=0.8$，MTTD 为 5 min，MTTR 为 25 min，计算得到积分项 $\int_{t_0}^{t_1} I(t)\,\mathrm{d}t \approx 0.667$。

（4）结论

SIEM 系统在异常行为发生后约 5 min 产生高危告警（MTTD=5 min），超出规定时间（3 min）。预设的 SOAR 剧本（自动阻断该运维账号的会话）成功执行，平均响应时间（MTTR）为 25 min。事件超时响应率为 66. 67%。

3. 3　评测结果与分析

根据实验结果，得出该系统的数据安全能力体系失效风险为：

$$\mathrm{Risk}=0.3\times22.2\%+0.3\times7.1\%+0.4\times66.67\%=0.355$$

本次实验有效地识别出该测试业务系统多个安全短板，验证结果有效推动了该系统在权限申请逻辑的优化、API 安全网关策略的强化以及应急响应预案和自动化剧本等方面的加固。数据安全有效性验证前后关键指标对比如图 3 所示。

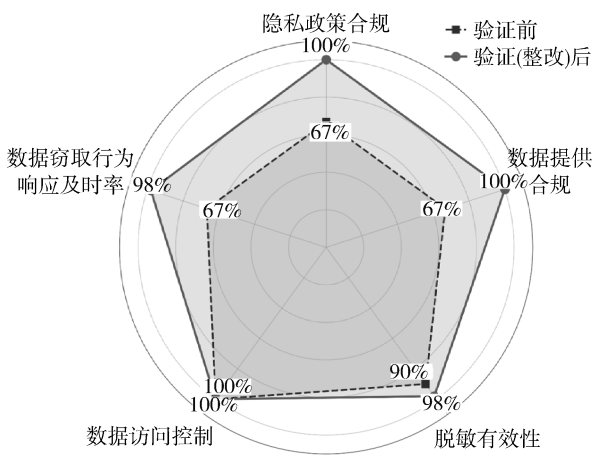

图 3　数据安全有效性验证前后关键指标对比

评测结果表明，该验证体系能够在以下几个方面帮助企业：

（1）精准定位安全短板：从合规、技术、事件三个维度全面、深入地发现潜在风险，将模糊的安全状态显性化为具体的数值。

（2）驱动安全能力闭环：验证发现的问题直接转化为可跟踪、可验证的整改任务，形成了“验证-发现-整改-再验证”的 PDCA（Plan-Do-Check-Act）闭环，有效推动了数据安全治理体系的实质性提升。

（3）量化安全价值：将安全工作的成效通过 MTTD、MTTR、RTO 等关键指标进行量化呈现，为安全决策和资源投入提供了强有力的数据支撑，使安全

价值更加显性化。

4 结论

本研究针对数据安全领域缺乏系统性的有效性验证方法这一问题，提出“三域一体”数据安全有效性验证方法论，建立了一套动态的、可量化的、贴近实战的闭环验证机制。通过将抽象的安全要求转化为具体的验证指标和流程，使得该方法论能够系统性地评估数据安全体系的真实防护能力，为电信运营商乃至更广泛的数据密集型行业的安全治理提供了科学的工具。该框架可根据技术发展进一步深化和拓展：

智能化与自动化：随着人工智能技术的发展，可以探索利用 AI/ML 技术赋能验证过程。已有研究表明，AI 驱动的安全验证在电信领域具有巨大的应用潜力[17]，例如，利用 AI 智能生成更优的攻击路径、根据环境变化自适应调整验证策略，以及通过分析历史验证数据来预测性地发现潜在安全风险。

与隐私增强技术（Privacy-Enhancing Technologies，PETs）的结合：随着同态加密、联邦学习、差分隐私等隐私增强技术的逐步应用，如何设计有效的验证方法来度量这些技术在实际应用中的安全性、隐私保护强度和性能开销，将是一个重要的研究方向。

参考文献

[1] 中国信息通信研究院. 大数据白皮书(2020 年)[R/OL]. (2020-03-27). http://www.caict.ac.cn/english/research/whitepapers/202003/P020200327550643303469.pdf.

[2] 王丹阳, 侯宁. 数据要素市场建设中的企业数据合规分析[J]. 信息通信技术与政策, 2023, 49(4): 42-47.

[3] DigitalDefynd. 5 telecom cybersecurity case studies [2025][EB/OL]. (2025-07-31). https://digitaldefynd.com/IQ/telecom-cybersecurity-case-studies/.

[4] European Parliament and Council of the European Union. Regulation (EU) 2016/679 (General Data Protection Regulation)[S/OL]. (2016-05-04). https://gdpr-info.eu/.

[5] 全国网络安全标准化技术委员会. GB/T 35273-2020 信息安全技术 个人信息安全规范[S]. 北京: 中国标准出版社, 2020.

[6] Alevizos L, Ta V T. Threat-informed cyber resilience index: a probabilistic quantitative approach to measure defence effectiveness against cyber attacks[J]. arXiv preprint arXiv:2406.19374, 2024.

[7] Ahmad A, Maynard S B, Desouza K C, et al. How can organizations develop situation awareness for incident response: a case study of management practice[J]. Computers & Security, 2021, 101: 102122.

[8] Roy P, Chandrasekaran J, Lanus E, et al. A survey of data security: practices from cybersecurity and challenges of machine learning[J]. arXiv preprint arXiv:2310.04513, 2023.

[9] Buck C, Olenberger C, Schweizer A, et al. Never trust, always verify: a multivocal literature review on current knowledge and research gaps of zero-trust[J]. Computers & Security, 2021, 110: 102436.

[10] Bernardo L, Malta S, Magalhães J. An evaluation framework for cybersecurity maturity aligned with the NIST CSF[J]. Electronics, 2025, 14(7): 1364.

[11] 王小乾. 数据要素合规流通的风险评估与防范[J]. 信息通信技术与政策, 2024, 50(4): 41-46.

[12] Gavric N, Shalaginov A, Andrushevich A, et al. Enhancing security in international data spaces: a STRIDE framework approach[J]. Technologies, 2025, 13(1): 8.

[13] Maiga A A, Ataro E, Githinji S. Balancing data privacy and 5G VNFs security monitoring: federated learning with CNN+BiLSTM+LSTM model[J]. Journal of Electrical and Computer Engineering, 2024: 1-16.

[14] Palma A, Bartoloni N, Angelini M. BenchIMP: a benchmark for quantitative evaluation of the incident management process assessment[C]//Proceedings of the 19th International Conference on Availability, Reliability and Security (ARES 2024). ACM, 2024: 1-12.

[15] Matheu S N, Martínez-Gil J F, Bicchierai I, et al. A flexible risk-based security evaluation methodology for information communication technology system certification[J]. Applied Sciences, 2025, 15(3): 1600.

[16] Fei Yuan, Yin Jiaqi, Yan Lijun. Security verification framework for NDN access control[J]. Scientific Reports, 2025, 15(1).

[17] 5G Americas. Advances in trust and security in cellular wireless networks in the age of AI[R]. 2025.

（收稿日期：2026-04-03）

作者简介：

张侃（1970-），男，博士，教授级高级工程师，主要研究方向：信息通信、网信技术等。

刘坚桥（1993-），通信作者，男，硕士，主要研究方向：通信领域网络安全运营、数据安全治理等。E-mail：18979177887@chinatelecom.cn。

刘孝颂（1977-），男，学士，高级工程师，主要研究方向：网络安全运营、重大任务网络安全保障等。

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