引用格式：卢超，刘婷，王璇璇. 考虑网络风险放大效应的责任式创新协同机制研究——以工业母机数据安全为例[J]. 技术经济，2026，45(5)：76-91.

Lu Chao，Liu Ting，Wang Xuanxuan. The responsible innovation collaboration mechanism considering network risk amplification：Evidence from the data security in machine tools[J]. Journal of Technology Economics，2026，45(5)：76-91.

考虑网络风险放大效应的责任式创新协同机制研究

——以工业母机数据安全为例

卢 超[1]，刘 婷[1]，王璇璇[2]

（1. 上海大学管理学院，上海 200444；2. 武汉大学经济与管理学院，武汉 430072）

摘 要：工业母机被视作“强国之基”，其数据安全因技术漏洞的网络风险放大效应而面临着日益严峻的次生破坏威胁，亟待以负责任的态度审视其技术创新。基于责任式创新理论，构建工业母机厂商、客户企业和政府的三方演化博弈模型，探究多主体协同治理工业母机数据泄露风险的动态演化规律。研究发现：在风险放大效应影响下，客户企业的责任式创新行为受次生破坏风险感知的显著正向影响，工业母机厂商的责任式创新行为受“市场倒逼”与“政策牵引”双重驱动，而政府监管遵循“市场自律替代”逻辑。研究进一步通过仿真证明，风险损失的规模变化会显著影响主体策略的收敛速度，当经济声誉损失或次生破坏损失突破关键阈值后，责任式创新行为将迅速内生化并主导系统演化。研究结论为工业母机数据安全治理提供理论支撑与实践路径，并对智能制造领域的责任式创新发展具有重要参考价值。

关键词：责任式创新；工业母机；数据安全；网络风险放大效应；次生破坏

中图分类号：F273.1；TP311 **文献标志码**：A **文章编号**：1002-980X(2026)05-0076-16

DOI：10.12404/j.issn.1002-980X.J25110202

一、引言

工业母机作为“强国之基”，被视作继集成电路之后第二个亟待啃下的“硬骨头”。当前，智能制造是中国建设制造强国的主攻方向，是事关国家经济安全和国防安全的战略性产业，对经济社会全局和长远发展具有重大引领作用[1]，而工业母机是发展智能制造的基础，数控机床作为工业母机的“大脑”，更是高端装备制造业价值链和产业链的核心[2]。高端数控机床融合新一代人工智能、工业互联网、工业大数据等新兴技术，形成的智能装备和智能制造生态系统[3]，被视为打造工业强国、占领国际竞争制高点的战略抓手，广泛应用于高端芯片、航空航天、车辆制造等关系国防安全、经济安全和社会安全领域的精密加工生产，其生产加工涉及众多企业工艺数据及国家机密信息[4]。

随着新一代信息技术在高端装备智能制造过程中的广泛应用，数控机床联网运行已成为趋势[5]，但由于数控系统技术前期设计、配置或协议上的缺陷，技术本身存在不可控的漏洞、后门等不利特性[6]，带来的安全隐患越来越突出。此外，工业母机行业具有显著的技术集中特征，其核心控制系统和关键模块长期由少数厂商主导，一旦技术漏洞在创新阶段被发现，便可能在产业链中形成规模化扩散。同时，工业母机作为制造业的基础装备，其安全风险具有明显的纵向传导特征，下游企业对其存在高度依赖，使得风险一旦发生

收稿日期：2025-11-02

基金项目：国家自然科学基金面上项目“责任式创新的触发机理与驱动机制：政府与企业、公众互动的视角”(72174116)；国家自然科学基金面上项目“基于负责任创新的‘AI+’产业融合互动机理与敏捷治理机制研究”(72574137)；上海市曙光计划“新兴技术扩散的责任治理机制研究——以自动驾驶为例”(24SG37)；上海市2025年度高水平机构建设运行计划“软科学研究”青年项目“上海‘AI+生物医药’融合的潜在风险与敏捷治理策略研究”(25692114100)

作者简介：卢超(1986—)，博士，上海大学管理学院教授，研究方向：创新管理与政策、管理理论与方法；刘婷(2000—)，上海大学管理学院硕士研究生，研究方向：创新管理与决策；王璇璇(1999—)，武汉大学经济与管理学院博士研究生，研究方向：供应链管理。

难以通过市场机制迅速消解，从而放大其社会与经济后果[7]。例如，2022 年，名为 Sality 的软件恶意利用可编程逻辑控制器（PLC）漏洞，破解了欧姆龙、西门子等知名品牌 PLC 口令，对设备所在企业实施勒索；2023 年，美国海军战舰造船厂遭勒索攻击，数控机床停机数天、上万人信息泄露；2024 年，钛合金叶片工艺窃密事件中攻击者长期潜伏在某航空制造企业的数控系统，完整窃取了军用发动机叶片加工轨迹、刀具补偿参数等关键工艺数据，造成价值 17 亿元的知识产权泄露。由此可见，以数控机床为代表的工业母机产业遭遇数据泄露事件，不仅影响工业母机设备制造行业本身发展，也会涉及产业链下游客户企业生产中断、工艺泄露及供应链连锁冲击等，甚至危及到国家机密数据安全。工业母机的漏洞信息通过产业链上下游快速扩散，引发次生损害，产生网络风险放大效应机制。而工业母机作为制造业源头的“制器之器”，应对技术创新中平衡责任、削弱网络放大效应进而减少次生破坏成为迫切需求。

责任式创新扎根于一个由企业、用户、政府等利益相关者组成的创新生态系统，每个利益相关者都发挥着作用并承担相应的责任，进行前瞻性协同决策[8]，引导技术创新朝满足伦理道德要求与社会需求的方向演进[9]。工业母机的数据安全问题与责任式创新理论具有天然的耦合性。一方面，工业母机的技术复杂性使得其漏洞风险具有强外部性，厂商的技术缺陷可能通过产业链传导引发“多米诺骨牌”效应，亟须在创新过程中嵌入前瞻性责任评估；另一方面，其数据安全涉及国家安全、企业商业秘密与个人隐私等多维度伦理边界，单纯依赖技术防御或政府监管难以奏效，亟须构建多方共治的责任分配体系。

基于上述分析，从责任式创新的视角，探究工业母机数据安全的多主体协同治理机制，考虑工业母机厂商、客户企业和政府三方主体的有限理性，运用演化博弈的方法探索三方主体协同治理数据泄露问题的动态演化特征，以期回答以下核心研究问题：政府、工业母机厂商与客户企业在有限理性下如何动态调整策略以实现演化稳定？网络风险放大效应与次生破坏如何影响多主体协同机制的设计？

二、文献综述

（一）责任式创新

“数智”时代，新兴技术负外部性的影响日益凸显，引发了公众对技术创新的关注与担忧[10]。责任式创新是一种多主体协同决策的动态过程，通过前瞻性治理评估创新条件、目标与结果，引导科技发展符合社会期望与伦理规范[9]。与传统创新范式相比，责任式创新嵌入在政府、企业、高校、科研机构、消费者等多主体构成的生态系统，强调协同决策与责任共担[11]，更关注技术风险、社会需求、道德伦理等[12-13]。

既有研究主要围绕理论阐述与实证分析展开，Stahl[11]将其应用于创新生态系统，提出责任式创新体系的概念，探讨人工智能伦理框架下的负责任创新。Zhang 等[14]开发了组织层面的责任式创新量表并加以验证。张秀娥等[15]基于资源编排理论，构建了绿色创业导向对企业责任式创新影响的实证研究模型。在责任式创新协同机制研究方面，曹霞等[16]探讨了企业主导、政府牵引和深度协作三种模式下的多主体责任式创新行为。Jia 等[17]以中国垃圾焚烧发电项目为例，构建了政府、废弃物焚烧企业及公众的博弈模型，探讨多主体策略在负责任创新中的机制。卢超等[18]以新冠肺炎疫苗为研究对象，分析了企业、消费者和政府等多主体在责任式创新过程中的演化博弈规律，为推动医疗技术的科技向善提供理论依据。虽然已有文献探讨了多主体之间的责任式创新协同机制，但更多是探究企业、个体公众和政府等主体间的动态演化，并未涉及上下游企业间的责任式创新协同，且均未考虑到网络环境下技术的风险放大效应及其可能引致的次生破坏，而这正是“数智”时代特别需要考虑的。工业母机作为“制器之器”，其创新如果不负责任，必然会引发企业用户“器”的问题。因此，本文研究对象包括工业母机产业链的上游制造厂商和下游应用企业，拓展了责任式创新的主体边界与风险情境。

（二）网络风险放大效应与次生破坏

风险放大指信息在传播过程中风险信号被增强[19]。次生破坏指间接造成的、派生的，由原生破坏引发的衍生破坏[20]。祝阳和雷莹[21]指出网络环境下微量风险信息可通过传播产生巨大社会影响，并引发次生危害。随着数字技术深度融入社会，网络安全风险被不断放大，次生破坏呈现出随网络扩张和蔓延的新特征，不仅涉及传统安全领域，更呈现出转向网络威胁等非传统安全领域的发展态势[22]。网络安全事件不仅

会导致企业运营中断和财务损失,更侵蚀企业声誉,削弱利益相关者信任[23-24]。耿勇等[25]指出网络安全事件不仅会对公司本身造成恶劣影响,还会波及客户与供应链。Pang 和 Fan[26]揭示了网络拓扑对系统性风险传播的重大影响。张才师和刘益[27]指出企业社会责任的体现是应对网络安全风险的一项重要策略。Zhu等[24]基于美国上市公司数据的分析表明,企业社会责任有助于预防和缓解数据泄露影响。

随着网络安全隐患不断涌现,网络监控、黑客攻击等频发给国家和社会造成信息安全威胁[22],衍生出一系列次生破坏。而工业母机作为“制器之器”,如果无法降低智能技术的负外部性,生产出的机器也会产生巨大危害,对产业链造成除运营中断等显性成本外,更会影响消费者的数据安全,对企业经济声誉等造成极大的次生破坏[23]。因此,考虑以工业母机为代表的智能制造设备,研究其技术漏洞因网络安全问题引致的风险放大效应和次生破坏至关重要,促进工业母机产业在拥抱数字化的同时坚持负责任创新,已成为产学界关注的紧迫议题。

(三)工业母机与数据安全

目前关于工业母机的研究多围绕“卡脖子”技术识别、竞争力评价、创新演化趋势等展开。贺远琼等[28]通过对华中数控的案例分析,探讨了在突破“卡脖子”技术过程中技术与市场创新的演进路径及互动关系。高道斌等[29]探究数控机床领域关键核心技术的识别体系与方法,提出一种结合双层技术结构与综合特征评估体系的识别方法。刘云等[30]分析了中国高端数控机床的创新发展进程和创新政策,指出其自主创新的起步、核心技术的突破和重点领域示范应用的创新发展趋势。Labucay[31]探究了工业母机在数字化转型过程中的可持续性,并确定其核心技术路径,构建了工业母机的技术创新体系。

但在数据安全方面,更多是定性分析工业母机网络安全的重要性,尚未展开责任式创新机制的探讨。Posada 等[32]指出物联网、工业大数据等智能制造技术伴随着众多信息安全风险,明确了数据安全在智能制造中的关键作用。Rahman 和 Shafae[33]指出操作技术与信息技术融合在促进制造业发展的同时,也增加了网络攻击风险,一旦突破纯网络防御,将导致经济损失并危及人身安全。董悦等[34]概述了数控机床在工业互联网环境下遭遇的系统设计缺陷、预留后门、数控协议等安全问题。其中,工业母机安全漏洞是指在数控系统的软硬件、通信协议等方面或安全策略方面存在的一些缺陷。Edward[6]曾指出制造商前期研发时无法完全避免技术漏洞,提出漏洞是导致威胁潜在发生的一个不利特性。赖英旭等[35]指出攻击者可以利用漏洞缺陷获得某些系统权限,对系统执行非法操作,从而导致数据泄露,造成严重财产损失和机密信息泄露。

通过梳理文献发现,目前责任式创新相关研究多聚焦政府、企业与公众等主体,较少将其引入工业母机等关键智能制造装备领域,对产业链上下游企业协同的刻画较少。此外,对于网络风险放大效应研究多停留在宏观风险传播或企业个体影响层面,同时现有工业母机研究则主要关注技术突破与创新发展,对数字化转型中数据安全风险的治理机制缺乏定量分析。基于此,在现有研究的基础上,将责任式创新理论拓展至智能制造场景,聚焦工业母机产业链上下游企业及政府等多主体,在纳入网络风险放大与次生破坏因素的基础上,研究其协同决策与行为演化。

可能的创新点有:第一,区别于以往责任式创新机制研究多考虑企业、终端个体用户与政府的传统设计,本文研究企业用户,可以拓展上下游企业协同实施责任式创新的理论体系;第二,考虑工业母机存在技术漏洞的不利特性和数据泄露的网络风险放大效应,探讨工业母机厂商、客户企业和政府在有限理性下行为的演化规律与稳定策略,拓展了责任式创新理论的风险情境。

三、模型假设与构建

构建工业母机数据安全协同治理的三方演化博弈模型,各主体之间的逻辑关系如图1所示。其中,客户企业是指购买和使用工业母机设备的下游用户企业,如汽车企业、航空航天企业、船舶企业等。客户企业不仅是消费端的购买者,同时也是市场监督者[36],在设备使用过程中通过漏洞检测与追责维修实现市场监督功能,与政府的监管角色形成互补。工业母机厂商实施责任式创新是指厂商事前加大技术研发投入以减少漏洞出现概率,并积极修复补丁、加强技术全过程漏洞审查和升级维护保障等。客户企业参与责任式创新指企业进行技术评估和安全审查与追责,如增加侦测设备的无线电信号监测,能够发现漏洞并要求厂商对

设备维护升级，出于审慎性原则会通过网络隔离、定时开关机生产等[7]手段避免漏洞被利用。政府在责任式创新中提供激励政策和监督管理[37]，并进行包容审慎性执法。《中华人民共和国科学技术进步法》中指出对探索性强、风险高的科学技术研究开发项目，科学技术人员已经履行了勤勉尽责义务仍不能完成的，予以免责。工业母机作为高端制造的核心装备，其研发涉及机械设计与制造、电气控制与自动化等多学科交叉领域，研发过程中需要攻克众多前沿科学问题和技术难题。但由于工业母机存在技术漏洞的不利特性[6]，即使厂商负责任地进行技术创新，尽到了当时科学技术水平和合理注意义务，设备仍有可能存在漏洞缺陷，即仍存在漏洞概率，政府会免除对已履行责任式创新的工业母机厂商的惩罚。因此，政府强监管指政府采取奖励和处罚措施，鼓励工业母机厂商和客户企业进行责任式创新，对实施和参与责任式创新的工业母机厂商和客户企业予以补贴奖励，出于“尽职免责”原则仅对不实施责任式创新的工业母机厂商予以惩罚。弱监管指政府对工业母机厂商和客户企业不作奖惩措施[38-39]。

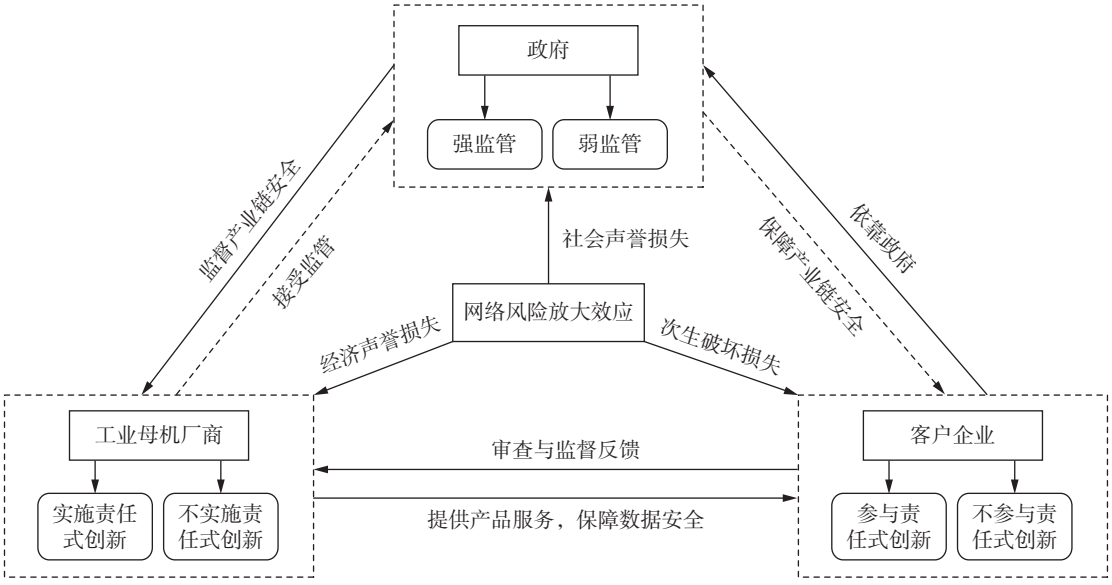


图1　三方演化博弈模型

（一）模型假设

假设1：在工业母机的数据安全治理过程中主要有政府、工业母机厂商、客户企业三个关键主体，均为有限理性，为追求利益最大化随时间不断调整策略选择。假设工业母机设备存在的漏洞会被攻击利用，并发生数据泄露现象。为简化分析并突出核心机制，将工业母机厂商的行为抽象为二元策略选择，将网络风险放大效应视为情境参数。

假设2：工业母机厂商的策略空间为（实施，不实施），选择实施责任式创新的概率为 $x(0\leqslant x\leqslant 1)$，选择不实施的概率为 $1-x$；客户企业的策略空间为（参与，不参与），选择参与责任式创新的概率为 $y(0\leqslant y\leqslant 1)$，选择不参与的概率为 $1-y$；政府的策略空间为（强监管，弱监管），选择强监管的概率为 $z(0\leqslant z\leqslant 1)$，选择弱监管的概率为 $1-z$。

假设3：工业母机厂商运营的基本收益为 R_m[40]，当工业母机厂商实施责任式创新时，投入成本为 C_m，能获得政府强监管下的补贴 S_m，实施后产品安全性能得到提高，降低了漏洞产生的概率。但由于数控系统技术漏洞的不利特性[6]，仍存在漏洞隐患的概率为 $a(0<a<1)$[41]。当客户企业参与责任式创新时，投入成本为 C_e，能获得政府强监管下的奖励 S_e，由于客户企业会加强设备安全性监测，能前瞻性地感知到安全隐患风险，识别出设备漏洞的概率为 $b(0<b<1)$[41-42]。当工业母机实施责任式创新时，出于“尽职免责”原则，厂商可免于政府的罚款，若客户企业参与责任式创新能够监测出设备漏洞并追责，此时网络风险放大效应引致的工业母机厂商的经济声誉损失为 abD_m。当工业母机厂商不实施责任式创新时，会受到政府强监管时的罚款 K_m，若客户企业参与责任式创新能够监测出设备漏洞并追责，工业母机厂商的经济声誉损失为 bD_m[43]。

假设 4：当客户企业参与责任式创新时，若工业母机厂商实施责任式创新，客户企业能获得工业母机厂商带来的长远安全收益$(1-a)R_e$[18]，但即便设备安全性能提高，由于漏洞的不利特性和风险的纵向传导性，会给客户企业带来包括生产中断、工艺泄露及供应链连锁冲击等次生破坏为$a(1-b)B_e$[33,44]。若工业母机厂商不实施责任式创新，给客户企业带来的次生破坏为$(1-b)B_e$。当客户企业不参与责任式创新，将不会投入成本来保障数据安全，此时若工业母机厂商实施责任式创新，客户企业能获得工业母机厂商带来的长远安全收益$(1-a)R_e$，但即便设备安全性能提高，由于漏洞的不利特性和网络风险放大效应，给客户企业带来的次生破坏为aB_e。若工业母机厂商不实施责任式创新，由于工业母机智能互联的特征和网络风险放大效应，给客户企业带来的次生破坏将达到最大B_e。在实际工业场景中，风险事件暴露往往会强化企业风险感知，并通过市场压力与声誉约束反向影响企业策略选择及漏洞发生概率。基于此，在后续分析中，通过改变由网络风险放大效应引致的损失参数，对“风险冲击—风险感知—策略调整”的内生演化趋势进行刻画，以在保持模型简洁性的同时反映风险-行为的反馈特征。

假设 5：当政府强监管时，将付出成本C_g，对实施责任式创新的工业母机厂商予以补贴S_m，对参与责任式创新的客户企业予以奖励S_e，若工业母机厂商和客户企业都参与责任式创新，会极大提高产业安全、社会稳定和国家信息安全，给政府带来额外的社会效益R_g[18]，在发生数据泄露时，出于“尽职免责”原则，政府仅对不实施责任式创新的工业母机厂商予以罚款$K_m(K_m>C_g)$[45]。当政府监管较弱时，若工业母机厂商和客户企业都参与责任式创新，给政府带来额外的社会效益R_g。当工业母机厂商实施且客户企业参与责任式创新时，由于漏洞的不利特性和网络风险放大效应，数据泄露给政府带来的声誉损失为$a(1-b)B_g$，在工业母机厂商实施且客户企业不参与时，政府损失为aB_g，在工业母机厂商不实施且客户企业参与时，政府损失为$(1-b)B_g$，工业母机厂商不实施且客户企业不参与时，政府损失将达到最大B_g。

所构建模型的主要参数设置及其含义见表 1。

表 1　参数设置及其含义

参数	定义
C_g	政府强监管的投入成本
R_g	政府在工业母机厂商和客户企业都参与责任式创新时获得的额外社会效益
S_m	政府强监管时对实施责任式创新的工业母机厂商的补贴
S_e	政府强监管时对参与责任式创新的客户企业的奖励
K_m	政府强监管时对不实施责任式创新的工业母机厂商的罚款
B_g	网络风险放大效应引致的政府的社会声誉损失
R_m	工业母机厂商的基本收益
C_m	工业母机厂商实施责任式创新的投入成本
R_e	工业母机厂商实施责任式创新带给客户企业的长远安全收益
D_m	网络风险放大效应引致的工业母机厂商的经济声誉损失
C_e	客户企业参与责任式创新的投入成本
B_e	网络风险放大效应引致的客户企业的次生破坏损失
a	工业母机厂商实施责任式创新时设备出现漏洞的概率
b	客户企业参与责任式创新时识别出设备漏洞的概率
x	工业母机厂商实施责任式创新的概率
y	客户企业参与责任式创新的概率
z	政府强监管的概率

（二）模型构建

根据上述假设，构建政府、工业母机厂商与客户企业的三方演化博弈矩阵见表 2。

表 2　政府、工业母机厂商与客户企业的收益矩阵

		工业母机厂商	客户企业	
			参与 y	不参与 $1-y$
政府	强监管 z	实施 x	$-C_g+R_g-S_m-S_e-a(1-b)B_g$	$-C_g-S_m-aB_g$
			$R_m-C_m+S_m-abD_m$	$R_m-C_m+S_m$
			$-C_e+S_e+(1-a)R_e-a(1-b)B_e$	$(1-a)R_e-aB_e$
		不实施 $1-x$	$-C_g-S_e+K_m-(1-b)B_g$	$-C_g+K_m-B_g$
			$R_m-K_m-bD_m$	R_m-K_m
			$-C_e+S_e-(1-b)B_e$	$-B_e$
	弱监管 $1-z$	实施 x	$R_g-a(1-b)B_g$	$-aB_g$
			$R_m-C_m-abD_m$	R_m-C_m
			$-C_e+(1-a)R_e-a(1-b)B_e$	$(1-a)R_e-aB_e$
		不实施 $1-x$	$-(1-b)B_g$	$-B_g$
			R_m-bD_m	R_m
			$-C_e-(1-b)B_e$	$-B_e$

四、模型分析

（一）工业母机厂商的策略稳定性分析

工业母机厂商实施责任式创新的期望收益为 E_x，不实施责任式创新的期望收益为 E_{1-x}，平均期望收益为 $\overline{E_1}$。

$$E_x = zy(R_m - C_m + S_m - abD_m) + z(1-y)(R_m - C_m + S_m) + (1-z)y(R_m - C_m - abD_m) + (1-z)(1-y)(R_m - C_m) \tag{1}$$

$$E_{1-x} = zy(R_m - K_m - bD_m) + z(1-y)(R_m - K_m) + (1-z)y(R_m - bD_m) + (1-z)(1-y)R_m \tag{2}$$

$$\overline{E_1} = xE_x + (1-x)E_{1-x} \tag{3}$$

因此，工业母机厂商的复制动态方程为

$$F(x) = \frac{dx}{dt} = x(E_x - \overline{E_1}) = x(1-x)(E_x - E_{1-x}) = x(1-x)[-C_m + z(K_m + S_m) + yb(1-a)D_m] \tag{4}$$

$$\frac{dF(x)}{dt} = (1-2x)[-C_m + z(K_m + S_m) + yb(1-a)D_m] \tag{5}$$

$$Q(z) = -C_m + z(K_m + S_m) + yb(1-a)D_m \tag{6}$$

根据微分方程稳定性定理，工业母机厂商实施责任式创新的概率处于稳定状态必须满足：$F(x) = 0$ 且 $dF(x)/dx < 0$。令 $Q(z) = 0$，可得当 $z = \dfrac{C_m - yb(1-a)D_m}{K_m + S_m}$ 时，$dF(x)/dx = 0$。

命题 1：工业母机厂商实施责任式创新的概率随着客户企业参与责任式创新和政府强监管概率的增大而上升。

命题 1 表明，当客户企业积极参与责任式创新时，工业母机厂商实施责任式创新的概率上升，客户企业深度参与能显著推动工业母机厂商对设备安全隐患的重视，进而积极采取措施来降低风险，从而促进了工业母机数据泄露的协同治理。当政府积极进行强监管时，工业母机厂商实施责任式创新的概率上升，政府通过补贴和罚款形成的奖罚机制，能够显著提高工业母机厂商的责任式创新动力。

命题 2：工业母机厂商实施责任式创新的概率与厂商经济声誉损失、客户企业参与责任式创新能识别出漏洞的概率呈正相关，与厂商实施责任式创新的成本、厂商实施责任式创新仍存在漏洞的概率负相关。

（二）客户企业的策略稳定性分析

客户企业参与责任式创新的期望收益为 E_y，不参与责任式创新的期望收益为 E_{1-y}，平均期望收益为 $\overline{E_2}$。

$$E_y = zx[-C_e + S_e + (1-a)R_e - a(1-b)B_e] + z(1-x)[-C_e + S_e - (1-b)B_e] + (1-z)x[-C_e + (1-a)R_e - a(1-b)B_e] + (1-z)(1-x)[-C_e - (1-b)B_e] \tag{7}$$

$$E_{1-y} = zx[(1-a)R_e - aB_e] - z(1-x)B_e + (1-z)x[(1-a)R_e - aB_e] - (1-z)(1-x)B_e \tag{8}$$

$$\overline{E_2} = yE_y + (1-y)E_{1-y} \tag{9}$$

因此，客户企业的复制动态方程为

$$F(y) = \frac{dy}{dt} = y(E_y - \overline{E_2}) = y(1-y)(E_y - E_{1-y}) = y(1-y)[bB_e - C_e - xb(1-a)B_e + zS_e] \tag{10}$$

$$\frac{dF(y)}{dt} = (1-2y)[bB_e - C_e - xb(1-a)B_e + zS_e] \tag{11}$$

$$P(x) = bB_e - C_e - xb(1-a)B_e + zS_e \tag{12}$$

根据微分方程稳定性定理，客户企业参与责任式创新的概率处于稳定状态必须满足：$F(y) = 0$ 且 $dF(y)/dy < 0$。令 $P(x) = 0$，可得当 $x = \dfrac{bB_e - C_e + zS_e}{b(1-a)B_e}$ 时，$dF(y)/dy = 0$。

命题3:客户企业参与责任式创新的概率随着工业母机厂商实施责任式创新概率的增大而下降,随着政府强监管概率的增大而上升。

命题3表明,当工业母机厂商积极实施责任式创新时,客户企业参与责任式创新的概率下降,在工业母机厂商积极采取负责任措施降低系统漏洞发生的情况下,能从源头避免数据泄露风险,客户企业自身参与的边际收益减少,会趋向于不参与责任式创新。当政府积极进行强监管时,客户企业参与责任式创新的概率上升,政府的奖励政策会促使客户企业主动参与责任式创新。

命题4:客户企业参与责任式创新的概率与政府奖励呈正相关,与自身参与责任式创新的成本呈负相关。

(三)政府的策略稳定性分析

政府强监管的期望收益为 E_z,弱监管的期望收益为 E_{1-z},平均期望收益为 $\overline{E_3}$。

$$E_z = xy[-C_g + R_g - S_m - S_e - a(1-b)B_g] + x(1-y)(-C_g - S_m - aB_g) + (1-x)y[-C_g - S_e + K_m - (1-b)B_g] + (1-x)(1-y)(-C_g + K_m - B_g) \tag{13}$$

$$E_{1-z} = xy[R_g - a(1-b)B_g] - x(1-y)aB_g - (1-x)y(1-b)B_g - (1-x)(1-y)B_g \tag{14}$$

$$\overline{E_3} = zE_z + (1-z)E_{1-z} \tag{15}$$

因此,政府的复制动态方程为

$$F(z) = \frac{dz}{dt} = z(E_z - \overline{E_3}) = z(1-z)(E_z - E_{1-z}) = z(1-z)[K_m - C_g - x(K_m + S_m) - yS_e] \tag{16}$$

$$\frac{dF(z)}{dt} = (1-2z)[K_m - C_g - x(K_m + S_m) - yS_e] \tag{17}$$

$$J(y) = K_m - C_g - x(K_m + S_m) - yS_e \tag{18}$$

根据微分方程稳定性定理,政府强监管的概率处于稳定状态必须满足:$F(z)=0$ 且 $dF(z)/dz<0$。令 $J(y)=0$,可得当 $y=\dfrac{K_m - C_g - x(K_m + S_m)}{S_e}$ 时,$dF(z)/dz=0$。

命题5:政府强监管的概率随着工业母机厂商实施和客户企业参与责任式创新概率的增大而下降。

命题5表明,当工业母机厂商实施责任式创新和客户企业参与责任式创新的程度增大时,政府的强监管概率下降,在工业母机厂商和客户企业积极采取措施加强数控系统漏洞防控和数据泄露风险分担情况下,会促进社会效益的提高,政府会降低监管的投入,更趋向于实施弱监管政策。

命题6:政府强监管的概率与工业母机厂商缴纳的罚款正相关,与强监管投入成本和给工业母机厂商的补贴负相关,与给客户企业的奖励关系受强监管投入成本、政府对工业母机厂商的奖惩力度影响。当政府对厂商罚款和补贴之差超过强监管成本的两倍时,政府强监管的概率与给客户企业的奖励负相关;当政府对厂商罚款和补贴之差小于强监管成本的两倍时,政府强监管的概率与给客户企业的奖励正相关。

(四)均衡点的稳定性分析

在演化博弈中,若博弈的均衡解达到演化稳定状态,那么该均衡解是严格纳什均衡,即属于纯策略均衡。因此,只需分析系统中8个纯策略均衡点的渐近稳定性即可。由 $F(x)=0$,$F(y)=0$,$F(z)=0$,可得8个纯策略均衡点:$E_1(0,0,0)$,$E_2(1,0,0)$,$E_3(0,1,0)$,$E_4(0,0,1)$,$E_5(1,1,0)$,$E_6(1,0,1)$,$E_7(0,1,1)$,$E_8(1,1,1)$。

将各个均衡点带入雅可比矩阵求对应的特征值,利用Lyapunov间接法分析各均衡点的稳定性,当特征值全为负时,该博弈均衡点为系统演化稳定点(ESS),均衡点的稳定性见表3。

命题7:当 $b(1-a)D_m - C_m < 0$,$C_e - bB_e < 0$,$K_m - S_e - C_g < 0$ 时,复制动态系统存在稳定点 $E_3(0,1,0)$。

命题7表明,当工业母机厂商实施责任式创新的投入成本超过其经济声誉损失、客户企业参与责任式创新的投入成本低于其网络风险放大效应引致的次生破坏损失、政府强监管成本超过对工业母机厂商的罚款

表 3　均衡点稳定性分析

均衡点	雅可比矩阵特征值		稳定性结论	条件
	$\lambda_1,\lambda_2,\lambda_3$	实部符号		
$E_1(0,0,0)$	$-C_m$, $-C_e+bB_e$, K_m-C_g	(−, ×, +)	不稳定	
$E_2(1,0,0)$	C_m, $-C_e+abB_e$, $-C_g-S_m$	(+, ×, −)	不稳定	
$E_3(0,1,0)$	$b(1-a)D_m-C_m$, C_e-bB_e, $K_m-S_e-C_g$	(−, −, −)	ESS	①
$E_4(0,0,1)$	$K_m+S_m-C_m$, $-C_e+bB_e+S_e$, C_g-K_m	(−, −, −)	ESS	②
$E_5(1,1,0)$	$C_m-b(1-a)D_m$, C_e-abB_e, $-C_g-S_e-S_m$	(−, −, −)	ESS	③
$E_6(1,0,1)$	$C_m-K_m-S_m$, $-C_e+abB_e+S_e$, C_g+S_m	(×, ×, +)	不稳定	
$E_7(0,1,1)$	$K_m+S_m+b(1-a)D_m-C_m$, $C_e-bB_e-S_e$, $C_g-K_m+S_e$	(−, −, −)	ESS	④
$E_8(1,1,1)$	$C_m-K_m-S_m-b(1-a)D_m$, $C_e-abB_e-S_e$, $C_g+S_e+S_m$	(×, ×, +)	不稳定	

注：-表示该特征值的符号为负，+表示该特征值的符号为正，× 表示该特征值的符号不确定；ESS 表示该点为系统的演化稳定点。① $b(1-a)D_m-C_m<0, C_e-bB_e<0, K_m-S_e-C_g<0$；② $K_m+S_m-C_m<0, bB_e+S_e-C_e<0$；③ $C_m-b(1-a)D_m<0, C_e-abB_e<0$；④ $K_m+S_m+b(1-a)D_m-C_m<0, C_e-bB_e-S_e<0, C_g-K_m+S_e<0$。

和对客户企业的奖励之差时，系统稳定于 $E_3(0,1,0)$。此时，工业母机厂商因实施成本过高，倾向于不实施责任式创新，客户企业因次生破坏损失过高，会选择主动参与责任式创新，政府因监管成本过高且客户企业自律性提升，趋向于弱监管。在工业母机产业中，该均衡点反映了“市场倒逼为主、政策干预为辅”的过渡阶段。中国工业母机产业中低端市场产能过剩，高端市场则面临“卡脖子”技术瓶颈，厂商因研发投入大、技术积累不足，实施责任式创新的成本显著高于其短期收益。与此同时，下游客户企业因直接承担数据泄露导致的次生破坏，风险感知强烈，往往主动加强安全审查与漏洞监测。政府在此阶段倾向于弱监管，实则是鼓励市场自律与用户监督相结合，避免过早干预抑制创新活力。

命题 8：当 $K_m+S_m-C_m<0$，$bB_e+S_e-C_e<0$ 时，复制动态系统存在稳定点 $E_4(0,0,1)$。

命题 8 表明，当工业母机厂商实施责任式创新的投入成本超过政府对工业母机厂商的奖惩之和、客户企业参与责任式创新的投入成本超过网络风险放大效应引致的次生破坏损失和政府对客户企业的奖励之和时，系统稳定于 $E_4(0,0,1)$。此时，政府的奖惩措施力度不足，尽管罚款额度超过监管成本，但厂商实施责任式创新的边际成本过高，而政府给予客户企业的奖励亦不足以覆盖其实施责任式创新的投入成本。因此，工业母机厂商、客户企业、政府分别选择不实施、不参与、强监管。此均衡点多见于工业母机产业标准化程度低、安全生态不完善的初期阶段。政府作为责任式创新的倡导者，试图通过奖惩机制引导责任式创新行为，而中国工业母机产业长期存在“重功能、轻安全”倾向，厂商因创新成本刚性对数据安全的投入意愿低，客户企业亦因风险认知滞后、技术能力不足而缺乏参与动力，市场主体缺乏主动参与的驱动力。

命题 9：当 $K_m+S_m+b(1-a)D_m-C_m<0$，$C_e-bB_e-S_e<0$，$C_g-K_m+S_e<0$ 时，复制动态系统存在稳定点 $E_7(0,1,1)$。

命题 9 表明，当工业母机厂商实施责任式创新的投入成本超过政府对其奖惩和工业母机厂商的经济声誉损失之和、客户企业参与责任式创新的投入成本低于客户企业的次生破坏损失和政府对客户企业的奖励之和、政府对不实施责任式创新的工业母机厂商的罚款超过监管成本和给予客户企业的奖励之和时，系统稳定于 $E_7(0,1,1)$。此时，政府通过优化客户企业奖励政策，显著提升客户企业参与积极性，但对工业母机厂商的奖惩力度仍未能抵消其创新成本与潜在损失的综合压力。因此，工业母机厂商、客户企业、政府分别选择不实施责任式创新、参与责任式创新、强监管。该均衡点刻画了在工业母机产业转型升级过程中，政府通过提高客户企业奖励，如安全审查补贴、税收优惠等，成功激发其参与责任式创新的积极性。然而，厂商因技术投入成本高、供应链协同难度大，仍处于观望状态。政府需通过链主企业牵头、配套资金跟随模式，推动形成客户需求拉动和厂商协同响应的创新生态。

命题 10：当 $C_m-b(1-a)D_m<0$，$C_e-abB_e<0$ 时，复制动态系统存在稳定点 $E_5(1,1,0)$。

命题 10 表明，当工业母机厂商经济声誉损失超过其实施责任式创新的投入成本、客户企业次生破坏损失超过其参与责任式创新的投入成本时，系统稳定于 $E_5(1,1,0)$。此时，工业母机厂商和客户企业的预期损失显著高于成本，将主动参与控制安全风险，政府的强监管措施因市场主体自律性增强而逐步退出，表明在工业母机数据安全协同治理过程中，政府通过前期政策引导构建了完善的责任共担机制，厂商负责任创

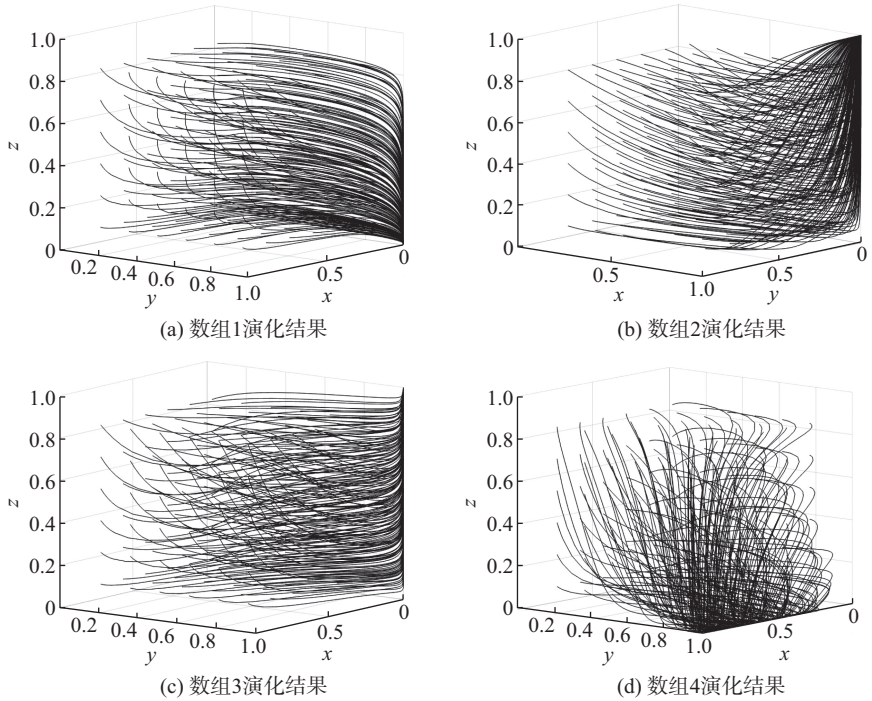
新意识与客户安全需求形成内生驱动力,责任式创新演变为行业常态。此均衡点是工业母机产业安全治理的理想状态,对应产业成熟期的高质量发展阶段。当厂商因品牌声誉、长期市场竞争力,将安全内置为技术基因,客户企业形成常态化安全审查能力,政府则逐步转向底线监管和标准服务。在此阶段,政府从直接干预者转向制度保障者,企业间协同效应显著提升,最终实现监管损失最小化与治理效能最大化。

五、数值模拟分析

为了探究前文稳定策略组合的演化稳定性及相关参数的敏感性,借助 MATLAB 软件进行仿真。

(一)演化策略稳定

为模拟系统的初始演化路径,需针对表 3 的系统演化稳定点进行参数赋值,但由于中国工业母机数据安全治理仍处于发展阶段,与本文研究主题直接相关的参数数据较为缺乏,且量纲统一的客观数据难以获得。由于参数赋值仅表示各变量之间的相对大小[46],参考相关研究[41,44,47],选择基于稳定性结果[48]的方式对各参数进行赋值,令满足条件①的数组 1 为:$K_m=32, S_m=10, S_e=5, C_g=30, C_m=80, D_m=40, C_e=50, B_e=100, a=0.3, b=0.6$;令满足条件②的数组 2 为:$K_m=40, S_m=10, S_e=5, C_g=30, C_m=80, D_m=40, C_e=70, B_e=100, a=0.3, b=0.6$;令满足条件④的数组 3 为:$K_m=50, S_m=10, S_e=15, C_g=30, C_m=80, D_m=40, C_e=30, B_e=100, a=0.3, b=0.6$;令满足条件③的数组 4 为:$K_m=60, S_m=10, S_e=28, C_g=30, C_m=40, D_m=100, C_e=15, B_e=100, a=0.3, b=0.6$。对四组数值分别从不同初始策略组合出发随时间演化 50 次,得到系统初设演化路径(图 2),数组 1 稳定于(不实施,参与,弱监管),数组 2 稳定于(不实施,不参与,强监管),数组 3 稳定于(不实施,参与,强监管),数组 4 稳定于(实施,参与,弱监管),仿真分析结论均与命题 7~命题 10 一致,说明结论有效。



(a) 数组1演化结果　(b) 数组2演化结果

(c) 数组3演化结果　(d) 数组4演化结果

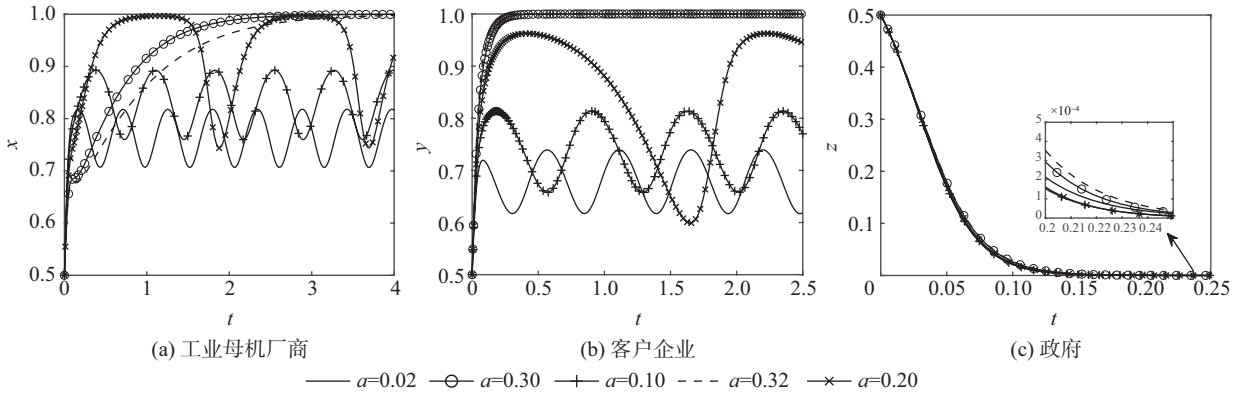
图 2　系统初始演化路径

(二)参数分析

从工业母机的创新发展过程来看,(1,1,0)是比较符合现实情况的选择,接下来在数组 4 的基础上,分别对参数 a、b、K_m、S_e、C_m、B_e、D_m 进行敏感性分析,探讨其对演化过程和结果的影响。

1. 工业母机厂商实施责任式创新仍存在漏洞概率的分析

令 $a=0.02, 0.1, 0.2, 0.3, 0.32$,仿真结果如图 3 所示。



(a) 工业母机厂商　(b) 客户企业　(c) 政府

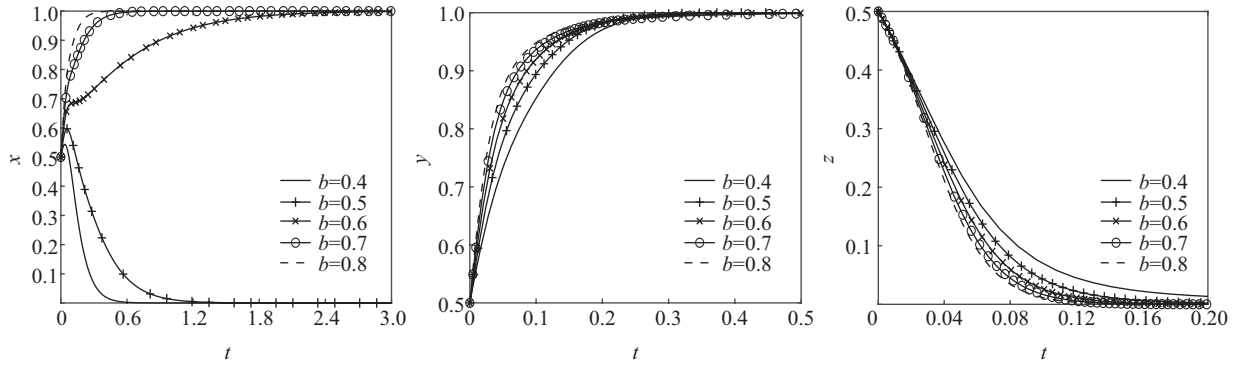
图 3　参数 *a* 的敏感性分析

图 3(a)表明,当漏洞概率极其小(如 $a=0.02$)时,工业母机厂商的演化轨迹表现出明显的波动性与不稳定性,其策略选择在较长时间内反复震荡,难以收敛至稳定均衡。这表明在责任式创新条件下,若存在漏洞概率非常低时,厂商在安全投入与创新收益之间面临较强的不确定性的权衡,其策略选择容易受到短期收益变化与外部反馈的影响,从而导致行为决策呈现出阶段性摇摆。随着漏洞概率增大,厂商策略的演化波动幅度明显减弱,当漏洞概率提升至 0.2 及以上时,厂商实施责任式创新策略逐渐表现出更强的收敛性,演化路径更快趋于稳定状态。这表明当漏洞概率上升时,潜在风险所带来的预期损失反而强化了厂商对系统性安全治理的重视,使其更倾向于持续实施责任式创新,从而稳定其策略。图 3(b)表明,在漏洞概率较小时,客户企业参与责任式创新的策略同样呈现周期性波动,反映出其对厂商安全承诺可信度的观望态度;而随着漏洞概率增大,客户企业对数据安全风险的感知增强,参与责任式创新的概率整体提高并趋于稳定。图 3(c)表明,政府策略对漏洞概率变化的敏感性相对较低,但在漏洞概率较大时,政府策略收敛于弱监管策略的速度减缓。该现象反映出在实施责任式创新背景下,仍存在的漏洞概率过低反而可能削弱厂商策略的稳定性,使其在短期收益与长期风险之间反复权衡;而当漏洞概率上升并被充分感知时,风险约束机制开始发挥作用,促使厂商、客户企业策略同步收敛。因此,行业技术进步与标准制定应致力于将漏洞概率控制在阈值以下,这是激发厂商内生动力的技术前提,厂商应从追求“零漏洞”转向构建“可度量、可迭代”的动态安全能力。例如,建立漏洞概率的实时监测与披露机制,向客户企业透明化展示安全绩效的边际改进。

2. 客户企业参与责任式创新识别出漏洞概率的分析

令 $b=0.4,0.5,0.6,0.7,0.8$,仿真结果如图 4 所示。

图 4(a)表明,当客户企业识别漏洞概率较低时,工业母机厂商收敛于不实施责任式创新策略,此时客户企业对漏洞识别能力有限,难以及时形成对厂商的有效约束;而当识别漏洞概率提升至 0.6 及以上时,厂商策略迅速向实施责任式创新收敛,表明客户企业识别能力的增强显著强化了对厂商的外部约束效应。



(a) 工业母机厂商　(b) 客户企业　(c) 政府

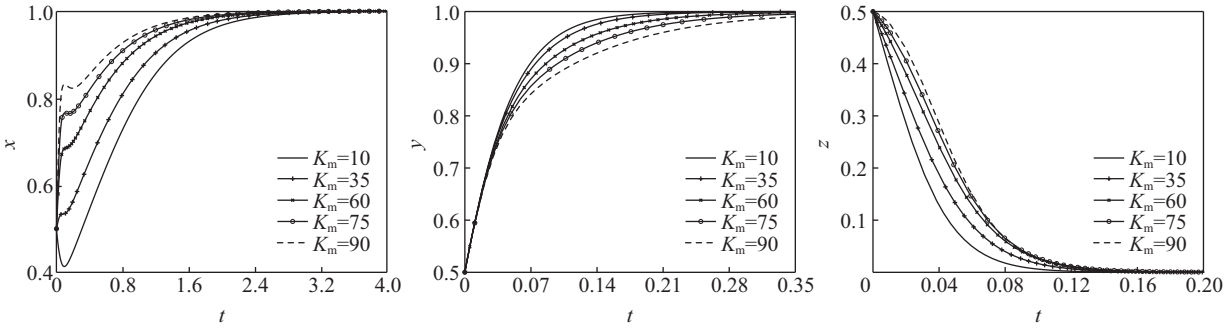
图 4　参数 *b* 的敏感性分析

图 4(b)表明,随着客户企业识别漏洞概率的变大,客户企业收敛于参与责任式创新策略的速度加快,较高的漏洞识别概率意味着客户企业能够更早发现潜在安全隐患,从而降低信息不对称程度,增强其参与责任式创新的内生动力。在此情形下,客户企业更倾向于主动参与协同治理,以降低数据泄露和次生破坏风险,其策略选择表现出更强的稳定性。图 4(c)表明,随着识别漏洞概率的提高,客户企业风险识别能力增强,市场主体间形成更为有效的自我约束机制,政府收敛于弱监管策略的速度加快,干预强度相应减弱。该现象揭示了客户企业漏洞识别能力的提升,不仅直接强化了客户企业参与责任式创新的意愿,也倒逼工业母机厂商提高安全治理水平,并在一定程度上替代外部监管职能。因此,客户企业可以通过培育安全检测机构、推广漏洞共测计划等措施,发挥市场倒逼作用,推动产业链内部形成稳定的协同机制。

3. 政府对不实施责任式创新的工业母机厂商罚款的分析

令 K_m = 10,35,60,75,90,仿真结果如图 5 所示。

图 5(a)表明,随着政府对不实施责任式创新的工业母机厂商罚款的变大,工业母机厂商收敛于实施责任式创新策略的速度显著加快。图 5(b)和图 5(c)表明,随着政府罚款的变大,客户企业收敛于参与责任式创新策略的速度减缓,政府收敛于弱监管策略的速度有明显减缓。这表明政府罚款具有强烈的政策牵引效应,罚款越大,厂商越倾向于通过责任式创新来避免处罚。但与此同时,客户企业在厂商逐渐改进的情况下,感知风险降低,从而减少了额外监督投入。政府则因维持罚款威慑而保持较高的监管力度,使得监管曲线下降趋势减缓。因此,政府的罚款策略需与补贴、声誉机制配合使用,避免形成长期惩罚依赖。



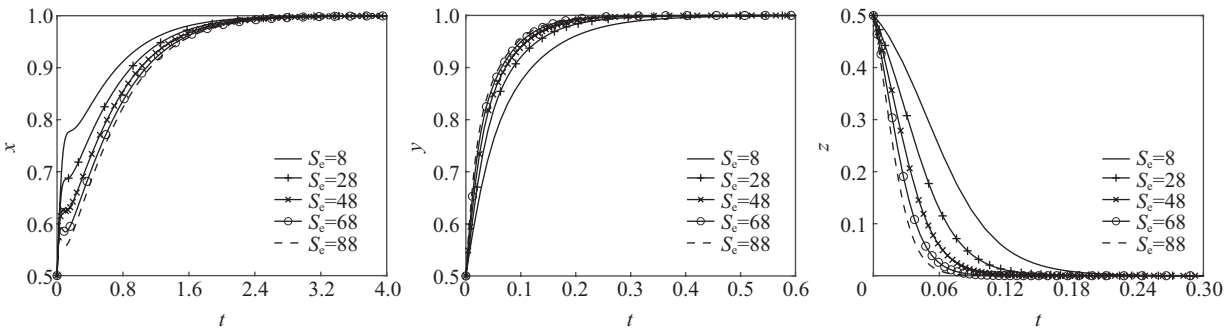
(a) 工业母机厂商　(b) 客户企业　(c) 政府

图 5　参数 K_m 的敏感性分析

4. 政府对参与责任式创新的客户企业给予奖励的分析

令 S_e = 8,28,48,68,88,仿真结果如图 6 所示。

图 6(a)表明,随着政府对参与责任式创新的客户企业奖励的变大,工业母机厂商收敛于实施责任式创新策略的速度减缓。图 6(b)和图 6(c)表明,随着政府对参与责任式创新的客户企业奖励的变大,客户企业收敛于参与责任式创新策略的速度加快,政府收敛于弱监管策略的速度显著加快。该现象揭示了奖励政策直接增



(a) 工业母机厂商　(b) 客户企业　(c) 政府

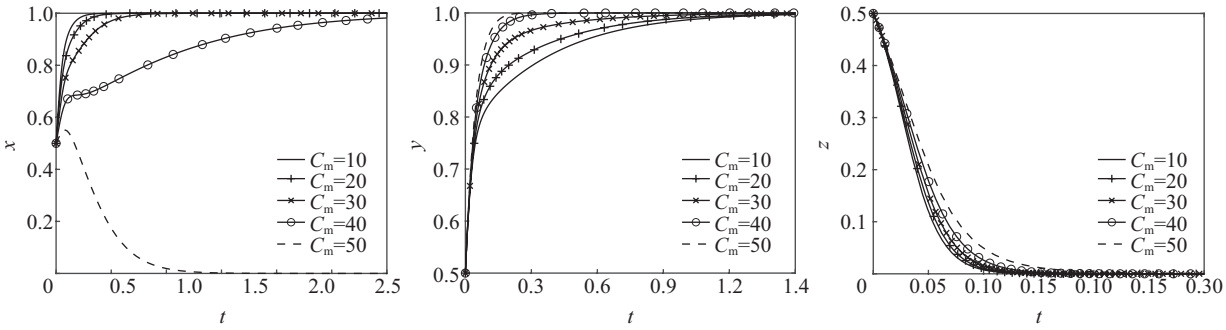
图 6　参数 S_e 的敏感性分析

强了客户企业的参与积极性，使其更愿意承担监督与风险管理的责任。而政府财政资源有限，对厂商的奖励就会减少，使得厂商责任式创新动力减弱。政府则因市场监督增强而更快地向弱监管收敛，降低了政策执行成本。因此，政府的奖励政策应注重结构性，可设计联合创新奖励，在激励客户的同时要求厂商协同投入。

5. 工业母机厂商实施责任式创新成本的分析

令 C_m = 10，20，30，40，50，仿真结果如图 7 所示。

图 7(a)表明，随着工业母机厂商实施责任式创新成本较低时，工业母机厂商倾向于选择实施责任式创新，且同一时刻成本越低，工业母机厂商选择实施的概率越高，但随着实施成本增大到超过阈值时，工业母机厂商会演化为不实施策略。图 7(b)和图 7(c)表明，随着工业母机厂商实施责任式创新成本的变大，客户企业收敛于参与责任式创新策略的速度显著加快，政府收敛于弱监管策略的速度减缓。该现象说明成本是影响厂商责任式创新行为的核心因素，当成本处于合理区间时，厂商具有积极性；但成本超过临界点后，厂商为规避高昂支出而选择不实施。客户企业在风险可能扩大的情况下，会加快参与以自我保护。政府因市场风险加剧而不得不维持一定的监管力度，导致弱监管的收敛速度下降。因此，政府可通过研发补贴、税收优惠、共性技术平台建设等方式，直接降低厂商的创新边际成本。



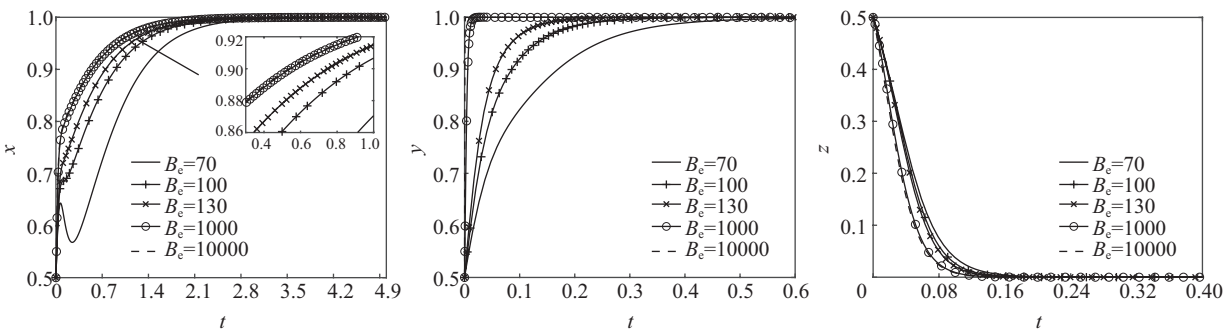
(a) 工业母机厂商　(b) 客户企业　(c) 政府

图 7　参数 C_m 的敏感性分析

6. 网络风险放大效应引致的客户企业的次生破坏损失的分析

令 B_e = 70，100，130，1000，10000，仿真结果如图 8 所示。

图 8(b)表明，客户企业的策略对次生破坏损失变化高度敏感，存在明显的量级效应。当次生破坏损失较低时，客户企业策略虽最终收敛，但调整过程相对平缓；而当次生破坏损失提升至千级及以上时，其参与责任式创新的概率迅速上升并快速稳定。这一结果表明，随着次生破坏损失不断扩大，客户企业对数据安全和系统性风险的感知显著增强，风险由潜在可能转变为现实威胁，从而将风险感知直接转化为参与责任式创新的行为动机。图 8(a)进一步显示，随着客户企业的次生破坏损失增大，工业母机厂商实施责任式创新策略的收敛速度加快，表明了当客户企业因网络风险放大效应而承受的次生破坏损失达到较高量级时，



(a) 工业母机厂商　(b) 客户企业　(c) 政府

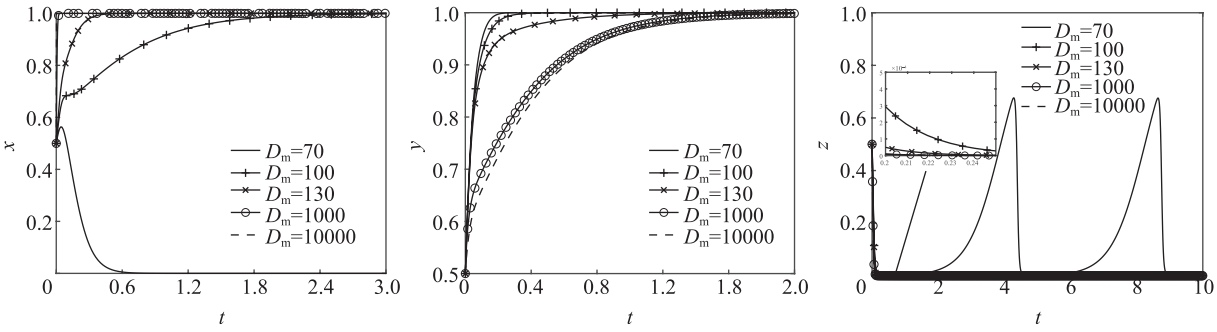
图 8　参数 B_e 的敏感性分析

潜在的连带责任压力和外溢风险显著增强，迫使工业母机厂商更快作出实施责任式创新的理性选择。图 8(c)表明，次生破坏损失变化对政府策略选择的影响不大，但当次生破坏损失变大时，客户企业会越重视数据安全，参与责任式创新的概率会变大，进而政府监管力度会变小。该现象揭示了当风险事件引致的次生破坏损失规模突破关键阈值后，风险感知显著增强，客户企业行为发生快速响应，进而通过责任式创新强化安全治理，同时对厂商形成压力，反向降低漏洞发生概率。同时，进一步揭示了网络风险放大效应通过影响企业风险认知与决策速度，内生塑造多主体协同治理路径。因此，政府与行业组织应加强风险警示教育，建立漏洞事件共享数据库，通过提升全行业风险感知来激活协同治理需求。

7. 网络风险放大效应引致的工业母机厂商的经济声誉损失的分析

令 D_m = 70，100，130，1000，10000，仿真结果如图 9 所示。

图 9(a)表明，随着工业母机厂商的经济声誉损失增大，其收敛于实施责任式创新策略的速度显著提升。当损失量级不足百级时，厂商策略收敛于不实施责任式创新，而当损失量级从百级突破至千级时，其策略在短时间内迅速趋于实施责任式创新，表明高额的经济声誉损失对厂商形成了强烈的约束作用。图 9(b)和图 9(c)表明，随着工业母机厂商的经济声誉损失增大，客户企业收敛于参与责任式创新策略的速度有所放缓，政府策略演化从一开始的不稳定波动，到逐渐收敛于弱监管策略。该现象揭示了当厂商自身受到的风险损失变大时，为避免品牌价值折损、客户流失及资本市场负面评价等长期代价，其主动实施责任式创新的内在动力显著增强。与此同时，由于厂商自律性提升，从源头降低了整体风险敞口，下游客户企业面临的可感知威胁相应减小，其投入成本进行额外监督和安全审查的边际收益下降，因此参与意愿放缓。对于政府而言，随着市场自我调节机制开始发挥作用，其直接行政监管的紧迫性与必要性降低。因此，必须强化并善用市场声誉机制，将其转化为驱动厂商责任式创新的核心杠杆。



(a) 工业母机厂商　　(b) 客户企业　　(c) 政府

图 9　参数 D_m 的敏感性分析

六、结论与启示

基于责任式创新理论，构建了政府、工业母机厂商与客户企业的三方演化博弈模型，探讨了工业母机数据安全协同治理的动态演化规律。研究发现：

第一，责任式创新的协同治理机制高度依赖于多主体间的动态博弈与策略调整。工业母机厂商责任式创新行为的演化遵循“市场倒逼”与“政策牵引”的双轮驱动机制，其实施责任式创新的概率与客户企业参与度和政府监管强度呈正相关。客户企业参与责任式创新意愿受网络风险放大效应下的次生破坏风险感知的显著正向影响，并受到工业母机厂商行为和政府激励的双重调节。政府的监管策略则随工业母机厂商和客户企业自律性增强而趋于弱化。工业母机厂商实施责任式创新的漏洞概率、客户企业参与责任式创新的风险识别概率和次生破坏损失及政府对工业母机厂商的罚款等显著影响演化结果，政府通过提高罚款和奖励力度可有效引导主体行为，但需平衡政策成本与激励效果。当工业母机厂商实施责任式创新的成本很高时，政府需要“下猛药”激励才能促进其实施责任式创新。当网络风险放大效应引致的客户企业次生破坏损失、工业母机厂商的经济声誉破坏规模很大时，风险由潜在威胁转化为显性约束，主体策略收敛速度显著加快。

第二，工业母机的技术漏洞存在着不利特性，其危害会通过产业链传导引发扩散，产业链中主体的收益和损失均会受到工业母机厂商实施时漏洞存在概率和客户企业参与时识别漏洞概率的影响，进一步揭示了以工业母机为代表的智能制造场景中风险放大的机制。即工业母机作为“制器之器”，其数据泄露不仅导致直接经济损失，更可能通过下游产业链引发国家安全层面的系统性危机。因此，在政策设计时需通过技术标准规制厂商降低漏洞概率，同时以产业链协同协议明确客户企业的监督责任，从而削弱网络风险放大效应引致的次生破坏的传导路径。

第三，系统存在的稳定均衡，揭示了工业母机数据安全治理的动态优化路径。对政府而言，需在治理初期构建“胡萝卜加大棒”的奖惩体系：一方面，通过财政补贴与税收优惠降低厂商的责任式创新投入成本和提高客户企业的风险感知与参与；另一方面，对不负责任的厂商实施高额罚款以形成威慑，可采取罚款机制，根据漏洞危害等级动态调整处罚力度。对工业母机厂商，需将责任式创新纳入技术研发核心流程，通过技术透明化提升客户企业信任，并建立漏洞披露与追溯机制以降低网络风险放大效应引致的次生破坏风险。对客户企业而言，则需强化数据安全能力建设，可利用区块链等技术实现供应链数据的实时审计，从而在降低自身损失的同时倒逼上游厂商履行责任。

此外，考虑到工业机器人、智能网联汽车等高度网络化、系统集成化的产业中，数据安全风险正呈现出与工业母机相似的放大特征，本文对其他相关智能制造领域同样有较好的参考价值和管理启示：第一，应将数据安全责任前移并嵌入技术创新全过程，引导设备制造商在系统架构设计、软件更新机制和漏洞响应流程中主动承担责任式创新义务，而非仅在风险暴露后被动补救；第二，应充分发挥使用方和市场机制的倒逼作用，通过合同约束、准入标准和声誉机制，将数据安全绩效纳入智能制造产品的核心竞争维度，促使制造商在高风险放大环境下形成内生治理动力；第三，政府监管应实施差异化干预，在高风险、高外部性场景中强化制度约束和激励引导，在风险可控阶段逐步推动多主体协同治理机制的形成。

本文仍存在一定局限。第一，模型将风险冲击主要作为情境参数处理，虽然通过概率和参数敏感性分析刻画“风险事件—风险感知—策略调整”内生影响，但未对风险冲击内生性进行显式建模。第二，模型中对厂商安全投入的渐进性进行了抽象处理，虽然较好地符合现实场景中的离散化决策行为，但未进一步刻画风险传导的级联放大机制。第三，现实中还存在信息不对称问题，如工业母机厂商可能隐藏技术缺陷，客户企业的风险感知亦可能存在识别滞后。未来研究可从两方面深入推进：第一，构建包含风险感知动态更新机制的多阶段或连续时间分析框架，将网络风险放大效应由外生冲击进一步内生化，刻画风险-行为的闭环反馈路径及其对协同稳定性的影响；第二，引入不完全信息与信号传递机制，探讨信息不对称、隐性缺陷披露与风险认知偏差对责任式创新协同治理的扭曲效应。

参考文献

[1] 高锡荣，丁洪伟，张红超. 智能制造的生产成本属性异变及边际成本递减律[J]. 技术经济，2024，43(7)：125-141.

[2] 翟晓荣，刘云，郭栋. 民营数控机床领军企业技术创新能力演进机制研究——昊志机电股份有限公司案例解析[J]. 科技进步与对策，2024，41(5)：140-149.

[3] 王磊，卢秉恒. 中国工作母机产业发展研究[J]. 中国工程科学，2020，22(2)：29-37.

[4] 高伟，陈劲. 中国工业母机产业基础能力、国家产业治理结构共同演化与“链创耦合”机理研究[J]. 中国软科学，2023(12)：1-15.

[5] 杨善林，王建民，侍乐媛，等. 新一代信息技术环境下高端装备智能制造工程管理理论与方法[J]. 管理世界，2023，39(1)：177-190.

[6] EDWARD A. Fundamentals of computer security technology[J]. Computer Fraud & Security Bulletin，1994，9：18-19.

[7] 中国信息通信研究院，北京神州绿盟科技有限公司. 数控机床网络安全研究报告(2023年)[J]. 自动化博览，2024，41(3)：32-34.

[8] 卢超，姜珊珊，成奕颖，等. “明知而故犯”，还是“及时止损”？——考虑责任式创新的人脸识别技术公众接受度研究[J]. 技术经济，2025，44(6)：125-138.

[9] 梅亮，臧树伟，张娜娜. 新兴技术治理：责任式创新视角的系统性评述[J]. 科学学研究，2021，39(12)：2113-2120，2128.

[10] LARKIN D，JASPERSEN L，PANDZA K. Balancing anticipatory and deliberative governance in public-private partnerships for responsible innovation：The role of corporate innovation capabilities[J]. Organization Studies，2025，46(9)：1257-1281.

[11] STAHL B C. Responsible innovation ecosystems：Ethical implications of the application of the ecosystem concept to artificial intelligence[J]. International Journal of Information Management，2022，62：102441.

[12] SOVACOOL B K，HESS D J，CANTONI R. Energy transitions from the cradle to the grave：A metatheoretical framework integrating responsible innovation，social practices，and energy justice[J]. Energy Research & Social Science，2021，75：102027.

[13] FISHER E. Engaging with societal challenges in responsible innovation[J]. Journal of Responsible Innovation, 2022, 9(1): 1-5.
[14] ZHANG S X, CHEN J, HE L, et al. Responsible innovation: The development and validation of a scale[J]. Technovation, 2023, 124: 102754.
[15] 张秀娥, 滕欣宇, 王超. 绿色创业导向对企业负责任创新的影响研究[J]. 科研管理, 2026, 47(2): 107-115.
[16] 曹霞, 李玮佳, 邢泽宇, 等. 责任式创新多主体合作机制[J]. 系统管理学报, 2024, 33(6): 1521-1539.
[17] JIA Y, ZHANG K, JIA Y. A tripartite evolutionary game analysis on China's waste incineration projects from the perspective of responsible innovation[J]. Energy Reports, 2023, 10: 1169-1181.
[18] 卢超, 邢窈窈, 蒋璐. 责任式创新的多主体演化博弈研究——以新冠疫苗研发为例[J]. 中国管理科学, 2023, 31(1): 226-237.
[19] 张群祥, 王成军, 邹琳. 互联网时代农产品质量安全事件风险是如何被放大的？——基于"速生鸡"事件的扎根分析[J]. 宏观质量研究, 2021, 9(1): 69-79.
[20] 陈长松, 陆虎成. "网络爆破"的特征、危害与治理初探[J]. 教育传媒研究, 2023(5): 69-71.
[21] 祝阳, 雷莹. 网络的社会风险放大效应研究——基于公共卫生事件[J]. 现代情报, 2016, 36(8): 14-20.
[22] 陈文旭. 21 世纪全球公共危机治理新挑战及中国智慧[J]. 湖南大学学报(社会科学版), 2021, 35(6): 7-14.
[23] KAMIYA S, KANG J K, KIM J, et al. Risk management, firm reputation, and the impact of successful cyberattacks on target firms[J]. Journal of Financial Economics, 2021, 139(3): 719-749.
[24] ZHU W, LI W J, WANG L. The impact of environmental, social, and governance ratings on corporate innovation: From the perspective of informal institutions[J]. Managerial and Decision Economics, 2024, 45(4): 2000-2022.
[25] 耿勇, 向晓建, 万攀兵. 供应链信任衰退: 网络安全风险与企业贸易信贷[J]. 中国工业经济, 2024(5): 135-154.
[26] PANG C, FAN H. Risk amplification effect of multilayer financial networks: Feedback mechanism or cyclic structure? [J]. Economics Letters, 2024, 242: 111887.
[27] 张才师, 刘益. 网络安全风险与 ESG 投资——基于声誉保险机制的解释[J]. 外国经济与管理, 2025, 47(4): 3-20.
[28] 贺远琼, 刘路明, 田志龙, 等. "政产学用"如何驱动"卡脖子"技术的双核创新——基于华中数控的纵向案例研究[J]. 南开管理评论, 2025, 28(2): 16-29.
[29] 高道斌, 陈悦, 韩盟, 等. 融合双层技术结构与综合特征评估的关键核心技术识别——以数控机床领域为例[J]. 情报杂志, 2025, 44(2): 82-91.
[30] 刘云, 郭栋, 翟晓荣. 中国高端装备制造业创新发展演进特征与政策优化研究——以高档数控机床为例[J]. 科学学与科学技术管理, 2022, 43(8): 19-31.
[31] LABUCAY I. Is there a smart sustainability transition in manufacturing? Tracking externalities in machine tools over three decades[J]. Sustainability, 2022, 14(2): 838.
[32] POSADA J, TORO C, BARANDIARAN I, et al. Visual computing as a key enabling technology for industrie 4.0 and industrial internet[J]. IEEE Computer Graphics and Applications, 2015, 35(2): 26-40.
[33] RAHMAN M H, SHAFAE M. Physics-based detection of cyber-attacks in manufacturing systems: A machining case study[J]. Journal of Manufacturing Systems, 2022, 64: 676-683.
[34] 董悦, 王吉, 李艺. 工业互联网场景下数控机床网络安全威胁与防护[J]. 自动化博览, 2022, 39(9): 32-35.
[35] 赖英旭, 刘静, 刘增辉, 等. 工业控制系统脆弱性分析及漏洞挖掘技术研究综述[J]. 北京工业大学学报, 2020, 46(6): 571-582.
[36] 陈劲, 肖彬, 刘沐洋. 制造商和用户协同创新: 理论框架与研究展望[J]. 技术经济, 2025, 44(6): 40-53.
[37] 赵庆, 余梅, 李京, 等. 负责任创新: 实践与理论分析[J]. 科研管理, 2021, 42(11): 1-7.
[38] 朱立龙, 荣俊美, 张思意. 政府奖惩机制下药品安全质量监管三方演化博弈及仿真分析[J]. 中国管理科学, 2021, 29(11): 55-67.
[39] 王腾, 关忠诚, 郑海军. 政府干预下的创新联盟协同行为演化博弈分析——基于联盟分类视角[J]. 技术经济, 2023, 42(3): 102-113.
[40] 杨坤, 汪万, 胡斌. 全生命周期视阈下责任式创新的演化博弈及扩散机制研究[J]. 运筹与管理, 2021, 30(6): 103-110.
[41] 韩普, 顾亮, 叶东宇, 等. 奖惩视域下区块链政务数据共享演化博弈研究[J]. 管理工程学报, 2024, 38(4): 122-132.
[42] 陈衍泰, 郝亚杰, 衡予婧, 等. 动态能力视角下人工智能和人类智能融合应急管理决策机制研究——以突发性公共事件为例[J/OL]. 系统工程理论与实践, 1-20[2026-05-03]. https://link.cnki.net/urlid/11.2267.n.20240929.1102.015.
[43] 李晓娣, 原媛. 负责任创新的多主体随机演化博弈研究——以应对老年数字鸿沟为例[J]. 运筹与管理, 2023, 32(11): 124-131.
[44] 韩菁, 李松梅, 王九天. 多主体行为演化视角下责任式创新的长效机制研究[J]. 管理评论, 2024, 36(7): 155-167.
[45] SUN H, GAO G. Research on the carbon emission regulation and optimal state of market structure: Based on the perspective of evolutionary game of different stages[J]. RAIRO-Operations Research, 2022, 56(4): 2351-2366.
[46] 李柏洲, 王雪, 苏屹, 等. 中国战略性新兴产业间供应链企业协同创新演化博弈研究[J]. 中国管理科学, 2021, 29(8): 136-147.
[47] 王丹丹, 解世程, 程英英. 考虑信任损益的健康大数据开放利用演化博弈分析[J]. 图书情报工作, 2024, 68(19): 54-65.
[48] SHENG J, ZHOU W, ZHU B. The coordination of stakeholder interests in environmental regulation: Lessons from China's environmental regulation policies from the perspective of the evolutionary game theory[J]. Journal of Cleaner Production, 2020, 249: 119385.

The Responsible Innovation Collaboration Mechanism Considering Network Risk Amplification: Evidence from the Data Security in Machine Tools

Lu Chao[1], Liu Ting[1], Wang Xuanxuan[2]

(1. School of Management, Shanghai University, Shanghai 200444, China; 2. School of Economics and Management, Wuhan University, Wuhan 430072, China)

Abstract: As the backbone of advanced manufacturing, machine tools face growing data security risks due to secondary damage caused by the amplification of network threats. These challenges demand a responsible approach to technological innovation. Based on the theory of responsible innovation, an evolutionary game model involving machine tool manufacturers, client enterprises and the government was constructed, exploring the dynamic evolution of multi-stakeholder collaboration in mitigating data leakage risks. The findings reveal that under the risk amplification effect, client enterprises' responsible innovation behaviors are significantly positively influenced by perceived secondary risks, while manufacturers' responsible innovation is driven by the dual forces of "market-driven pressures" and "policy-induced incentives". Government regulation follows "market self-regulation substitution". Simulation results further indicate that the scale of risk losses significantly impacts the convergence speed of the main strategy. When economic reputation losses or secondary damage losses exceed critical thresholds, responsible innovation behavior rapidly becomes endogenous and dominates system evolution. It provides theoretical insights and practical strategies for improving data security governance in machine tools and contributes to the broader discourse on responsible innovation in intelligent manufacturing.

Keywords: responsible innovation; machine tools; data security; network risk amplification effects; secondary damage