物联网产品安全监管研究

谢志利[1,2] 李文昭[1,2]

（1.中国标准化研究院；2.国家市场监管重点实验室（产品缺陷与安全））

摘 要：当前，物联网正呈指数级增长。对于消费者而言，物联网提供了更多的产品选择、安全性、便利性和个性化。对于企业而言，增加了跨全球供应链跟踪产品的可能性。同时，物联网给产品安全也带来了新的挑战，对产品安全监管领域既有的制度体系提出了更高要求。本文基于物联网产品安全现状及其复杂性，结合传统产品安全监管手段，从消费品安全、数据安全和隐私之间的交叉性和相互依赖性出发，提出了物联网相关产品安全监管基本思路及相关监管工具。

关键词：物联网，产品安全，监管

DOI编码：10.3969/j.issn.1674-5698.2023.01.019

Research on the IoT Products Safety Regulation

XIE Zhi-li[1,2] LI Wen-zhao[1,2]

（1. China National Institute of Standardization;
2. Key Laboratory on Product Defect and Safety, State Administration for Market Regulation）

Abstract: At present, the Internet of Things (IoT) is growing exponentially. For consumers, the IoT provides more product choices, security, convenience and individualization. For enterprises, it increases the possibility of tracking the products of global supply chain. At the same time, the IoT also brings new challenges to product safety, and puts forward higher requirements for the existing system in the field of product safety regulation. Based on the current situation and complexity of IoT product safety, combined with traditional product safety regulation, this paper proposes the basic ideas and related regulation tools of IoT related products from the intersection and interdependence among consumer product safety, data security and privacy.

Keywords: Internet of things (IoT), consumer safety, regulation

1 物联网概述

在数字化革命驱动下，全球出现了新的数字消费市场，其中包括物联网（Internet of Things, IoT）。物联网本身不是一种产品，而是一种使联网产品具有新的功能的技术。这种技术涵盖连接或能够连接到互联网的产品，通过这种连接，产品的活动方式可被改变，包括潜在的安全性能。

物联网改变了很多消费者每天的工作和生活方式，允许消费者远程影响消费品的物理变化，使消费

基金项目：本文受中央基本科研业务费项目“全国产品缺陷与安全管理标准化技术委员会- 电动汽车电池管理系统无线短距通信功能安全要求研究-2022”（项目编号：282022Y-9464）资助。

作者简介：谢志利，硕士研究生，高级工程师，研究方向为产品安全与召回。

者的生活更轻松，风险更小，并提高了效率。物联网也改变了传统产品设计、制造和产品交付过程的监控、分析和改进方式，有助于企业更好地为客户提供新服务。例如：物联网能够帮助公司远程修复产品缺陷，包括主动限定产品召回范围，直接通知消费者产品召回，且补救措施可以自动推送到受影响的产品上，从而提高召回效率。

物联网分为工业物联网（与商业或工作场所相关）和消费物联网（与消费相关）。本文仅探讨消费领域的物联网产品。

2　物联网技术对产品安全的挑战

2.1　物联网产品潜在的安全危害

传统产品的危险通常是由于机械、热或电方面存在不合理危险，也可能是在设计者预期使用寿命结束以后仍在使用以及人为故意对安全功能的破坏等而产生的不安全情形。对于物联网产品，意外危险可能直接来自设备联网以及数据处理的不可见性。由于未经授权、不谨慎或异常数据传输或者操作代码的干扰或操纵，物联网产品变得危险，可能造成消费者伤害或死亡。在这种情况下，消费者往往无法预见因数据更改导致产品存在安全缺陷以及由此产生的危险状况。

物联网产品潜在的产品安全危害，主要包括以下4类：因软件更新导致的故障或性能变化导致的产品安全功能丧失、与互联网的连接丧失以及相应的功能丧失、用于支持安全功能的数据损坏以及可穿戴设备的潜在人身伤害。

（1）软件更新或修改导致的故障。物联网应用程序可能会出现故障，原因可能是产品销售时存在缺陷或不当软件更新以及被不法分子入侵。如果应用程序出现故障，可能会导致设备以未预料到且可能不安全的方式动作或反应，导致设备加速或减速，发生机械故障。

（2）网络连接丧失。如果产品依赖与物联网的连接来安全运行，且产品没有设计为在失去连接时进入安全模式，则可能会妨碍物联网设备或应用程序正常运行产生，产生潜在的安全影响。如果设备本身具有保护功能，保护系统因网络连接丧失而不能正常运行则问题将更为严重。

（3）数据质量和完整性问题。数据质量尤其是物联网的一个新问题，在安全功能依赖于某些数据的情况下，数据必须准确无误，否则安全功能可能无法运行。特别是当自动决策使用的数据来自没有可靠信誉的第三方时，如果数据不正确或具有误导性，可能会导致物联网设备和应用程序出现意外情况。

（4）人身伤害。物联网设备和应用在身体内、身体上或身体附近，如设备或应用中电池或其他反应材料有问题则会导致化学或热烧伤以及皮肤刺激，增强和虚拟现实设备可能导致眼睛疲劳、眼外伤、眼睛发育等问题。

2.2　对产品安全监管政策的挑战

2.2.1 基本概念的界定

（1）关于物联网产品。我国《产品质量法》第二条明确规定：“本法所称产品是指经过加工、制作，用于销售的产品。建设工程不适用本法规定；但是，建设工程使用的建筑材料、建筑构配件和设备，属于前款规定的产品范围的，适用本法规定。”此规定相当于界定了《产品质量法》规制的产品，属于动产，且应为“有形”产品，不包括服务。物联网设备或应用程序是产品和服务的混合体，涉及“硬件”和“软件”、“产品”和“服务”。“硬件”可被视为一个设备或一组设备或物理对象，这些设备或对象在本质上具有响应性，能够检索数据并按指示行事。“软件”是一组程序，可实现与硬件组件之间的数据收集、存储、处理、操作和指示。整体上来讲，物联网设备区别于将原材料、半成品经过加工、制作，改变形状、性质、状态，成为产品成品的情形，涉及包括作为智力成果的信息、数据等，提供的网络服务，以及作为共享的物联网设备等，比传统意义上的“产品”内涵要丰富得多。

（2）关于物联网产品安全。产品在合理正常或可预见的使用或滥用时对消费者的健康或安全造成不合理的风险时被认定为不安全，传统产品安全指产品不存在因机械接触、电能或热能释放或有毒暴露而导致的死亡、身体伤害的状态。物联网消费品具有动态性质，比如在投放市场时被认定为安全的产品因为通过软件升级或产品远程破解对产品代码作出变更使其变得不安全。这区别于传统意义上的

产品安全，即产品的不安全不是因为设计、制造方面的问题，而是由于未经授权或异常处理的数据而变得危险。

2.2.2 产品安全责任主体的界定

物联网环境下，涉及诸多参与者，例如：在自动驾驶车辆中，涉及车辆移动应用程序、传感器制造商，传感器网络运营商，道路运营商和提供软件的第三方等。产品和服务生产者、参与者相互依赖，物联网设备和应用程序通常根据其设计的性质，依赖第三方技术来执行其基本功能。如果应用于产品中的第三方软件在产品首次上市时没有缺陷，但产品投放市场后，由于第三方的更新（有时是在制造商不知道或无法控制的情况下），可能会改变产品的性能和安全性，产生意外的产品安全风险。尤其当产品的性能受到由人工智能产生的数据影响时，问题可能会更加复杂，因为人工智能依赖于来源广泛的大量数据。

针对上述物联网技术带来的新的监管问题，需要及时梳理和调整产品安全监管政策，既确保消费者能够从安全的物联网产品中获益，同时保障物联网市场健康发展。

3 物联网产品安全监管政策思考

3.1 基本思路

3.1.1 处理好产品安全与其他领域的交叉关系

传统上，产品安全、数据安全和隐私保护按照相关的法律法规分别由相应的监管机构负责。物联网环境下，数据安全、隐私保护和产品安全相互依存且交叉重叠。

物联网产品本质上是数字环境的一部分，其性能和功能受到软件的控制。在物联网产品中，存储在连接设备中或进出连接设备的所有数据均可能会影响产品的安全，包括操作说明（软件）；源自消费者的数据（如：生物特征、设置和偏好、多用户识别）；环境指标（如：位置、温度、大气、能源）等。数字安全问题对于确保产品安全和正常运行至关重要，因为这种数据安全会造成人身伤害，导致产品的某种不合理风险，所以物联网潜在危害不仅可能是一种数字安全风险，同时也是一种产品安全风险，从这个意义上讲，数据安全风险管理也是消费品安全的一部分，是产品安全政策应该考虑的一个重要问题。

物联网产品相关的潜在问题中，还涉及个人隐私问题。侵犯隐私本身不是产品安全问题，但侵犯隐私获得的信息可能被用于对消费者的健康或安全造成威胁。例如：对于儿童玩具和儿童保育设备，与儿童个人数据有关的数据保护和隐私问题，包括谁使用、谁有权访问以及出于何种目的等较为敏感和重要，因为这可能会带来安全问题。

物联网环境下，产品安全问题是独特的，需要特别考虑，产品安全监管机构不针对数据安全和个人隐私问题，但应关注数字安全风险如何影响产品安全。识别造成不合理人身伤害风险的潜在数据安全缺陷，并做出适当的反应，保护消费者的人身安全，这是物联网环境下产品安全监管应厘清和明确的基本原则。

3.1.2 促进产品安全监管和技术创新的平衡

在考虑现有的产品安全制度是否适合物联网时代的目的并作出政策调整时，需要在确保以下各项之间取得平衡：确保较高水平的消费品安全，同时避免不必要地扼杀创新，应能继续促进有助于提高产品安全性的新技术的发展。包括一方面要鼓励企业技术创新，引导企业就新技术应用主动查找问题，改进设计、制造，降低产品安全风险；另一方面，优化完善产品安全监管制度，尽早将这种新技术引发的安全问题纳入监管范围，更好地保护消费者合法权益。这需要探索物联网产品安全监管新型方式，更好地平衡技术创新和安全风险，推动产业健康安全有序发展。

3.1.3 加强国内外相关方合作

安全是物联网发展的最大优先事项之一。对数据和数据处理系统的保护构成网络安全，网络安全是国家重要战略之一，需要整体谋划和部署。通过产品安全监管也是发挥政府在网络安全战略作用的着力点，产品安全监管机构可考虑架构物联网产品安全协调中心，明确各机构在物联网产品安全方面的作用，加强机构间合作，例如：实现信息共享、共同制定标准、开展研究以及协调执法活动等。

政府和行业之间的持续密切合作对于寻求物联

网安全解决方案也很重要。政府需要与物联网相关各方密切合作，以了解与其应用相关的安全风险，并共享知识。通过政府和行业的共同努力，可以加快物联网安全方面的创新。

另外，此类技术的市场日益全球化，物联网跨国界运营，使得物联网超越了地理和政治边界，一些国际组织，如：经合组织（OECD）、国际消费品健康与安全组织（ICPHSO）、物联网创新联盟（AIOTI）等，已经展开大量国际层面的对话和协调，出台一些政策性文件，以确保消费者获得一致的安全。产品安全监管机构应充分利用这些平台，加强国际合作和对话，促进物联网安全监管方法的改进。

3.2 具体监管工具考虑

在相关政策工具上，可从以下几个方面考虑：市场准入，包括设置什么样的条件，谁应负责产品安全认证并保证合规；如何定义物联网产品的不合理危险；谁对产品安全负责；发生事故后采取什么措施以及如何向消费者传达安全信息等。

3.2.1 标准

一些现有的产品安全标准需要更新，设置互联网连接控制器的具体安全要求以及互联网连接控制系统测试，将互联网连接所带来的人身危害考虑进去；针对一些特殊产品，还要考虑国家和地方基础设施建设中的智能系统进行集成和非预期交互等问题。在制定物联网设备技术法规时，尽可能原则化，保持其足够的灵活性，以适应技术的变化。支持自愿性标准的制定，也可以考虑发布一些物联网产品安全的指导性文件等。

3.2.2 认证

如果要求对高风险物联网产品进行认证，需要考虑认证标准应适合具有类似功能或安全性能的特定类别的产品。还应考虑认证周期的问题。物联网中消费品安全相关的最大挑战是产品本身会随着时间而演化，制造商可能通过远程改善产品或修复漏洞或弱点，在这种动态的环境中，传统产品认证程序在评估及测试物联网产品对安全法规及标准合规性方面可能存在不合理性。例如：要求每次软件更新进行认证的话，过程过于缓慢、花费更多，更重要的是制造商无法快速响应技术快速变化的需求。在合规性方面，鉴于设备和应用程序之间的高度集成以及物联网生态系统的复杂性，特殊情形下可能需要确定最初应由谁认证产品的安全性和合规性、所需认证的范围以及负责的时间跨度等。

3.2.3 信息披露

物联网消费品市场中存在大量不对称信息，消费者很难了解他们购买产品安全性的所有技术细节，所以也很难估计这些产品的安全性。传统上，产品安全警告以纸质形式（包括产品标签）随产品一起交付给消费者。在物联网中，消费者与物联网设备的交互由远离设备的应用程序或基于软件的服务支持，因此产品制造商拥有前所未有的能够更快速、更有效地与用户的消费者群体建立联系的能力。制造商应使用更有效的方法向消费者提供关键安全警告和说明，在产品首次激活时以及产品的整个生命周期内，向消费者传达重要的安全信息。这可能包括告知安全安装和设置说明，在产品使用过程中不断提醒安全使用，更新安全说明，发布关于产品召回或安全修改的信息，以及有关维护要求和寿命终止问题的及时信息等。

3.2.4 信息收集

多渠道收集事故和伤害报告是产品安全监管工作的基础，传统上，监管机构通过消费者报告、医院伤害信息监测、企业报告、媒体报道等多渠道收集有关产品安全事件的信息。通过收集与消费品有关的伤亡数据以及暴露出来的危险方面的信息，同时调查特定的伤害案例获得有关伤害或危险以及涉及产品的更多信息，然后系统地进行分析，以确定存在的危险以及应对措施。目前，物联网安全相关信息并不是很多，但随着物联网产品的市场规模扩大，预计物联网设备安全报告数量会越来越多。监管机构应增强数据收集技术，以获取有关物联网产品安全的信息，除了传统的信息采集方式，特别是基于目前的网络安全技术，在网络安全监测中捕获相关产品安全事件可能是个有效的方式。

3.2.5 风险评估

传统的产品安全危害分析和风险评估工具已经成熟，如何基于前期成果评估物联网产品带来的潜在产品安全风险也是一个需要解决的问题。物联网环境下，风险评估应针对预期使用环境中的所有产品组件（包括机械硬件和软件组件）进行评估，包括

连接到产品的设备与其预期安装环境（车库、家庭、车辆、学校等）之间的热或动力学相互作用；由用户通过远程操控而对能量释放（热、电、动能）可能带来的后果；在预期和可预见的使用环境中，主体设备与其他物联网系统的非预期交互等等。

3.2.6 召回

一旦发现投放市场的物联网设备存在危及人身安全风险时，需要制造商实施召回，以保护消费者人身财产安全。具体召回措施上，除了传统意义上的修退换措施，对于软件或应用程序问题导致的缺陷，制造商还可以远程修复产品缺陷，并且补救措施可以自动推送到受影响的产品上，这有助于提高召回效率。由于确保及时向受影响的目标受众提供召回通知是召回的一个重要组成部分，所以要防止制造商通过互联网以软件更新的方式“私下”纠正有缺陷的产品，而没有通知公众，或者未向产品安全监管部门进行报告，这会限制召回的效果，关于这一点应在相关召回管理制度中予以明确。

3.2.7 消费者安全教育

除了及时发布产品召回信息，以解决迫在眉睫的安全隐患外，包括政府部门在内的各类组织和机构可通过开展一系列安全教育活动，提高消费者对与物联网产品相关的已经存在的、隐藏的以及正在出现的安全隐患的认识，帮助其获得相关信息，增强消费者的自我保护能力，降低死亡和受伤的风险。这可能需要开展有针对性的教育工作，通过用户指南和安全消费提示、具体案例等有效的方式，教育消费者学习了解物联网产品，使消费者了解潜在风险，鼓励消费者购买安全性强的产品等。

4 结语

中国正致力于实现高质量发展，物联网技术的发展将为经济社会发展注入新的动能，应把握好这一发展机遇，处理好与其相关的法律、安全、政府治理等方面的问题和挑战，发挥政府为新技术健康发展保驾护航的关键作用，确保消费者能够从安全的物联网产品中获益，同时不妨碍行业技术进步和创新。

参考文献

[1] 张树红. 基于物联网安全的研究[J]. 山西电子技术, 2022 (04):91–93.

[2] 尹钟舒,洛向刚,杨成,等. 物联网（IoT）: 国内现状和国家标准综述[J]. 网络安全技术与应用, 2022 (09):08–111.

[3] 陈钊,曾凡平,陈国柱,等. 物联网安全测评技术综述[J]. 信息安全学报, 2019 (05):3–16.

[4] 杨毅宇,周威,赵尚儒,等. 物联网安全研究综述: 威胁、检测与防御[J]. 通信学报, 2021 (8): 188–205.

[5] 周丽莎,孔勇平,陆钢. 物联网安全政策解读及技术标准综述[J]. 广东通信技术, 2017(12)·39–42.

[6] 张玉清,周威,彭安妮. 物联网安全综述[J]. 计算机研究与发展, 2017 (10) : 2130– 2143.

[7] 谷呈星,赵训威. 物联网的安全分析[J]. 科技创新与应用, 2022 (05):51–53.

[8] 刘念. 物联网的伦理争议及其应对策略——基于“万物皆媒”的理论假设[J]. 西部学刊, 2022 (7):62–65.

[9] 苏恺,郑华,李卢城,等. 物联网典型安全漏洞及其防护[J]. 数字技术与应用, 2022(04): 212–214.

[10] 刘奇旭,靳泽,陈灿华,等. 物联网访问控制安全性研究综述[J]. 计算机研究与发展, 2022(10):1–22.

[11] 钱萍,吴蒙. 物联网隐私保护研究与方法综述[J]. 计算机应用研究, 2013(01):13–20.

[12] 张夕夜,王亚楠. 主要国家物联网安全法律政策研究[J]. 信息通信技术, 2021(06): 13–17.