关于工业互联网数据安全解决思路的探讨

朱立锋
(中电工业互联网有限公司,北京 100190)

摘　要：介绍了我国工业互联网数据安全所面临的发展现状，从国际和国内两个方面分析了工业互联网数据安全所面临的问题，并从贯彻落实数据安全法律法规、建立健全数据安全组织体系以及建立自主可控的先进技术体系初步提出了工业互联网数据安全解决思路，为进一步提升我国工业互联网数据安全工作水平提供了参考。

关键词：工业互联网；数据安全
中图分类号：TN915.08　　**文献标识码**：A　　DOI：10.16157/j.issn.0258-7998.212508

中文引用格式：朱立锋. 关于工业互联网数据安全解决思路的探讨[J].电子技术应用，2022，48(2)：1-3.
英文引用格式：Zhu Lifeng. Discussion on industrial Internet data security solution[J]. Application of Electronic Technique，2022，48(2)：1-3.

Discussion on industrial Internet data security solution

Zhu Lifeng
(CEC Industrial Internet Co.，Ltd.，Beijing 100190，China)

Abstract：This article introduced our country industry development present situation，analyzed the problems of industrial Internet data security from both international and domestic aspects，and put forward solution for industrial Internet data security from the implementation of safety laws and regulations，establishing and improving the data security system and establishing an independent and controllable advanced technology system. It provides reference for further improving the level of industrial Internet data security in China.
Key words：industrial Internet；data security

0 引言

当前，世界新一轮科技革命和产业变革迅猛发展，工业互联网作为新一代信息技术与制造业深度融合的产物，作为以数字化、网络化、智能化为主要特征的关键基础设施，日益成为新工业革命的关键支撑，对未来工业发展产生全方位、深层次、革命性影响，对推进制造强国和网络强国建设，建设社会主义现代化强国具有重大意义。

工业互联网数据是指工业互联网这一新模式新业态下，在工业互联网企业开展研发设计、生产制造、经营管理、应用服务、供应链管理和物流管理等业务时，围绕客户需求、订单、计划、研发、设计、工艺、制造、采购、供应、库存、销售、交付、售后、运维、报废或回收等工业生产经营环节和过程，所产生、采集、传输、存储、使用、共享或归档的数据。如果按类型来划分，工业互联网数据主要包括工业互联网设备数据、应用系统数据、知识库数据、企业数据、用户个人数据五大类。

本文基于对工业互联网数据安全的发展现状、存在问题进行深入分析的基础上，提出解决工业互联网数据安全问题的基本思路。

1 发展现状

当前，社会各界围绕法律、制度、标准、技术等领域对工业互联网数据安全展开热烈讨论、积极探索，相关工作加速推进并取得了阶段性成果。

(1)法规政策加速完善。继 2016 年 11 月发布《网络安全法》以来，《数据安全法》《个人信息保护法》相继于 2021 年 6 月和 8 月审议通过，数据安全立法和法律实践稳步推进。具体到工业互联网领域，有关部门相继发布了《关于深化“互联网+先进制造业”发展工业互联网的指导意见》《加强工业互联网安全工作的指导意见》《工业互联网创新发展行动计划（2021-2023 年）》《关于工业大数据发展的指导意见》《工业数据分级分类指南(试行)》等一系列政策文件，为开展工业数据分类分级、管理能力评估、有序共享、治理与防护等相关工作提供了政策指导。

(2)标准建设稳步推进。2021 年 12 月，《工业互联网安全标准体系(2021 年)》正式发布，该标准体系包括分类分级安全防护、安全管理、安全应用服务等 3 个类别、16 个细分领域以及 76 个具体方向。在数据安全领域明确提出了《工业互联网企业数据安全防护要求》《工业互

联网重要数据识别指南》《工业互联网数据跨境安全防护要求》等标准，为切实发挥标准规范引领作用，加快建立数据安全分类分级管理制度，强化工业互联网企业数据安全防护能力，推动工业互联网产业高质量发展具有重要支撑作用。

(3)安全能力持续提升。产学研用各界围绕着工业互联网数据安全的基础通用技术、数据安全管理技术、数据安全防护技术以及涵盖数据的产生、传输、存储、处理、使用及销毁等数据全生命周期流转安全开展理论研究和技术攻关，随着区块链、多方安全计算、联邦学习以及数据沙箱等数据安全技术快速发展，以接入认证、访问控制、权限管理、网络隔离、数据加密、数据脱敏、数据备份和恢复等为代表的主要技术手段日趋成熟，“数据可用不可见”“数据不动程序动”等正加快从理念变为现实。

2 面临问题

随着工业互联网的迅猛发展，其所沉淀的数据体量不断增大、种类不断增多、结构日趋复杂，并逐渐向海量、多维和双向流动的改变。随之而来的数据安全问题也日益凸显，主要表现为数据泄露、非授权访问、用户信息泄露等方面。

从国际看，工业互联网数据安全形势严峻。

(1)网络攻击方式新型多样。暴力破解凭证、勒索攻击、撞库攻击、漏洞攻击等新型攻击方式层出不穷，针对电力、能源、航空、医疗等重点领域工业互联网的攻击事件大幅增加，导致相关行业企业内部重要数据、敏感信息频频泄露，工业互联网数据安全面临严重威胁。

(2)数据黑市交易触目惊心。以暗网数据交易、精准诈骗、撒网式诈骗等为主要特征的网络犯罪活动日趋规模化组织化集团化。随着工业企业加快推进上云、工业APP培育，海量工业数据向云平台汇聚，形成高价值的数据资源池，这些工业数据日益成为犯罪集团牟取利益的窃密目标。

(3)数据安全风险日益加剧。随着工业领域向互联开放发展，新一代信息技术的广泛使用，相关设备、平台、系统和应用实现在线化、网络化，以及供应链、物流链的高度协同，潜在的风险敞口增多。再加上工业互联网跨设备、跨系统、跨厂区、跨地区互联互通的特点，对数据全生命周期各环节的安全防护的时效性、复杂性要求较高，所面临的挑战也持续增加。

从国内看，工业互联网数据安全管理也存在一些不足。

(1)工业互联网数据安全责任体系尚未建立。主管部门、工业企业、工业互联网基础设施运营单位、工业互联网平台企业、工业互联网供应链(一般包含制造商、上下游供应商、零售商以及消费者)、物流链(包括海关、进出口商、物流企业)等多方主体在保护工业互联网数据安全方面的权责义务还不够清晰，工业互联网数据安全保护要求难以落实到位。

(2)工业互联网数据安全管理理念落后缺位。工业互联网数据相关企业安全意识较为薄弱，数据安全管理理念落后甚至缺位，尚未形成能有效处理工业互联网数据安全与数据流通核心矛盾的全局性、整体性、战略性数据安全核心理念，工业互联网数据安全防护缺少科学的理念指导。

(3)工业互联网数据安全技术能力亟待加强。相关企业数据安全核心技术产品研发不够，应对新型攻击防篡改、防窃取、防泄露的安全核心技术能力还不足，产业支撑力不强，工业互联网数据安全风险发现、实时告警、防护处置等能力建设还需进一步提升。

3 解决思路

与传统互联网安全相比，工业互联网安全具有三大特点：一是涉及范围广，网络攻击面持续扩大，可直达生产一线；二是造成影响大，一旦发生安全事件，影响严重；三是企业防护基础弱，整体安全保障能力有待进一步提升。因此，对工业互联网而言，安全是保障，要坚持系统思维，从制度、管理和技术等方面构建统筹协调、科学高效的数据安全体系，促进数据的安全流通与高效配置。

(1)贯彻落实数据安全法律法规。坚持依法治理，全面贯彻落实国家《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》等法律法规，《关于深化“互联网+先进制造业”发展工业互联网的指导意见》《加强工业互联网安全工作的指导意见》等国家政策，以及《工业互联网数据安全保护要求》《工业互联网重要数据识别指南》等行业标准，结合行业企业实际，制定数据安全保护实施方案和工作机制，强化制度执行，全面提升工业互联网数据安全保护的法治化水平。

(2)建立健全数据安全组织体系。建立健全权责明晰、分级管理的数据安全监督管理体系。明确工业互联网数据安全各主体的责权利，研究制定数据分类分级管理规范，将数据安全保护和监管管理要求融入工业互联网研发设计、生产制造、供应链管理和物流管理等多种场景，以高质量的数据安全保护确保工业互联网产业链供应链物流链安全稳定，防范数据跨境流动风险。融入数据采集、传输、存储、使用、交换、共享、公开、归档、删除等全生命周期各环节。在数据采集阶段，要保证数据的完整性、准确性和机密性，在数据传输阶段，要做好传输主体及节点的身份鉴别和认证，在数据存储阶段，要做好数据存储加密、数据备份和恢复等工作。在数据处理使用阶段，要做好数据访问控制和权限管理。

(3)建立自主可控的先进技术体系。聚焦工业互联网数据安全需求，采用自主可控的信创产品建设高安全标准的数据金库和数据要素操作系统，归集并存储核心数

据和重要数据，为数据元件的生产开发与流通提供支撑，实现数据的安全流通与高效配置。例如，中电互联依托中国电子 CPU、操作系统和内存三位一体的内生安全 PKS 体系，积极践行中国电子“关键数据入库，双向风险隔离、三级安全管控”的数据安全核心理念，建立安全先进绿色的数据治理底座，构建全栈式的数据安全技术体系，为数据安全保护提供了坚实的技术保障。

参考文献

[1] 国务院关于深化“互联网+先进制造业”发展工业互联网的指导意见[EB/OL].(2017-11-27)[2021-12-28].http://www.gov.cn/zhengce/content/2017-11/27/content_5242582.htm.

[2] 工业和信息化部，教育部，人力资源和社会保障部，等.关于印发加强工业互联网安全工作的指导意见的通知[EB/OL].(2019-07-26) [2021-12-28].http://www.gov.cn/xinwen/2019-08/28/content_5425389.htm.

[3] 工业和信息化部.关于工业大数据发展的指导意见[EB/OL].(2020-04-28) [2021-12-28].https://www.miit.gov.cn/xwdt/gxdt/sjdt/art/2020/art_a61849ebec144ebdb91fa9bc547-4554c.html.

[4] 工业互联网专项工作组.工业互联网创新发展行动计划(2021-2023 年)[EB/OL].(2020-12-22) [2021-12-28].http://www.gov.cn/zhengce/zhengceku/2021-01/13/content_5579519.htm.

[5] 工业互联网产业联盟、工业信息安全产业发展联盟、工业和信息化部商用密码应用推进标准工作组.工业互联网安全标准体系(2021 年)[EB/OL].(2021-12-9)[2021-12-28].https://www.miit.gov.cn/ztzl/rdzt/gyhlw/gzdt/art/2021/art_52d120b9266242dc8418d3f822979b8a.html.

[6] 工业和信息化部.工业数据分类分级指南(试行)[EB/OL].(2020-02-27)[2021-12-28].https://www.miit.gov.cn/jgsj/xxjsfzs/wjfb/art/2020/art_4a24ace1dd824fe8b4b449c4aad9338a.html.

[7] 清华大学，中国电子信息产业集团有限公司.2021 城市数据治理工程白皮书[Z].2021.

[8] 国家工业信息安全发展研究中心，工业信息安全产业发展联盟.工业互联网数据安全白皮书[Z].2020.

[9] 张雪莹，陈雪鸿，杨帅锋.工业互联网数据安全标准体系研究[J].网络空间安全，2019(10)：86-92.

[10] 张雪莹，杨帅锋，王冲华，等.工业互联网数据安全分类分级防护框架研究[J].信息技术与网络安全，2021，40(1)：2-9.

[11] 董悦，李艺，秦国英，等.工业互联网数据安全技术研究[J].信息通信技术与政策，2020(10)：38-41.

[12] 刘晓曼.浅谈工业互联网数据安全现状与形势[J].保密科学技术，2021(9)：9-14.

(收稿日期：2021-12-28)

作者简介：

朱立锋(1964-)，男，博士，研究员级高级工程师，主要研究方向：智能制造、工业互联网、数据治理、人工智能、区块链、信息安全、系统集成、产业标准化、产业投资。

扫码下载电子文档

版权声明