物流快递行业信息安全研究（2018）

中国电子技术标准化研究院　　浙江菜鸟供应链管理有限公司

2019 年 3 月

内容摘要

我国拥有 14 亿的人口，如何推动零售业持续、稳定、健康的发展是社会各界共同关心的课题。随着“互联网+”新零售概念不断深化，物流快递行业也迎来大发展，新一代信息技术成为物流快递行业重要的驱动力。在物流快递行业帮助“新零售”走完“最后一公里”的同时，也掌握了海量的用户数据，这使得物流快递行业信息安全治理变得极其重要。可以说，快递安全不仅是运输安全、货物安全，更重要的是信息安全。

本报告尝试通过定性与定量相结合的分析，勾画出国内物流快递行业信息安全态势全景图，提升政府、企业、消费者等相关方对物流快递行业信息安全形势的重视。同时，通过分享国内主要快递企业在防控信息安全风险方面的良好实践，总结梳理行之有效的攻防经验。在此基础上，本报告从完善政法环境、发挥企业主体作用、推动技术创新、促进行业合作等方面，提出物流快递行业加强信息安全建设的建议，倡导构建共建、共治、共享的物流快递行业信息安全生态。

版权声明

目 录

图目录

表目录

引 言

随着经济结构不断优化、发展质量不断提升，人民群众对更便捷更优质生活的追求愈发强烈。电子商务恰逢其时，蓬勃发展，世界正在变得越来越“扁平化”。作为电子商务重要支撑的物流快递行业迎来重大发展契机，也经历了快速增长。

今天，“互联网+”新零售热潮的迅猛袭来使快递从“小包裹”迈向“大物流”的路径渐明。物联网、人工智能、大数据、云计算等新一代信息技术的深度应用使物流快递行业从人力密集型向技术、资本密集型的趋势更加明显。物流快递行业的智能化、数字化转型不仅赋能产业自身发展，对拉动消费、提振经贸活动同样发挥着重要的支撑作用；另一方面，深度分析挖掘并合理利用物流快递行业信息数据，有助于更为科学全面地分析经济运行状况，为相关部门掌握经济发展脉络、精准制定产业政策提供决策依据。

机遇从来都与风险同行。物流快递行业的数字化转型必然伴随着信息安全风险。物流快递信息系统被攻击、侵入，信息数据被泄露、滥用，不仅会造成用户合法的信息权益受损，给用户带来财产损失甚至人身伤害，还会影响商家、快递企业的品牌和声誉，更有甚者会危及公众和社会安全。因此，全面分析评估信息安全风险、总结分享应对措施与攻防经验、研究提出风险防控建

议并形成切实可行的措施成为推进物流快递行业健康持续发展的题中应有之义，也是本报告编写之初衷。

一、物流快递行业迎来快速发展

物流快递行业是推动流通方式转型、促进消费升级的现代化先导性产业，在降低流通成本、支撑新型零售发展、服务生产生活、扩大就业渠道等方面发挥了积极作用，已成为我国国民经济的重要产业和新增长点。2017 年 2 月，《快递业发展“十三五”规划》正式发布，为物流快递行业的发展谋划了蓝图。未来，物流快递行业将从扩大产业规模转向提高产业发展质量和效益。

1.1 物流快递行业发展总体情况

今天，我国快递行业已常态化进入单日快递“亿件时代”。可以说，快递行业与亿万人民群众的日常生活息息相关。如图 1 所示，过去几年中，物流快递行业无论是业务量还是业务收入都在迅速增长。2018 年，全国快递服务企业业务量累计完成 507.1 亿件，同比增长 26.6%；实现业务收入 6038.4 亿元，同比增长 21.8%。[1]

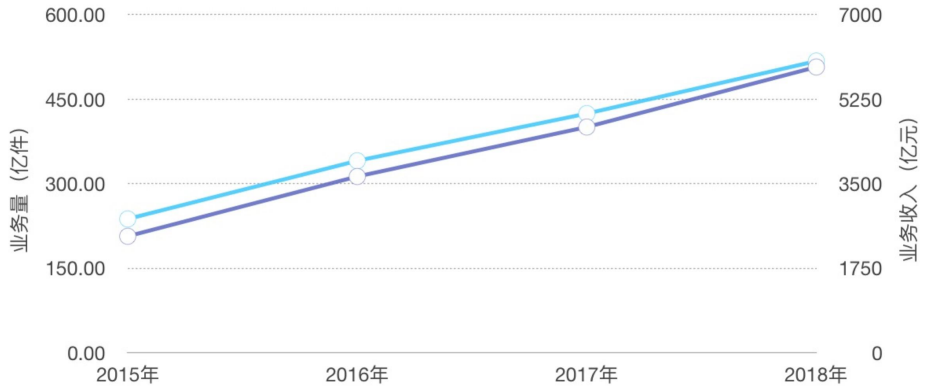

图 1 2015-2018 全国快递行业运行情况

[1] 数据开源：中华人民共和国国家邮政局

从区域上来看，华东、华南以及京津冀仍是快递业务集中的区域。除中西部的成都和武汉外，业务量和业务收入全国排名前十的均为华东、华南以及京津冀城市（见表 1）。

表 2 2018 年快递业务量及业务收入排名前十城市

排名	城市	业务量（万件）		排名	城市	业务收入（万元）
1	广州市	506447.8		1	上海市	10202806.0
2	金华（义乌）市	366123.2		2	广州市	4797456.2
3	上海市	348648.8		3	深圳市	4357146.7
4	深圳市	320825.6		4	北京市	3310328.2
5	杭州市	258910.0		5	杭州市	2966169.2
6	北京市	220875.6		6	金华（义乌）市	1699417.6
7	东莞市	133853.6		7	东莞市	1669023.1
8	苏州市	124563.0		8	苏州市	1557928.9
9	成都市	104785.4		9	成都市	1121953.5
10	泉州市	97247.4		10	武汉市	927295.2

目前，我国快递企业超过 2 万家，从业人员达到 300 万，各类营业网点达到 21.7 万处，在实现城市全覆盖的同时，快递乡镇网点覆盖率超过 86%，全行业日均服务突破 3 亿人次[2]。如此大的快递网络为电子商务发展提供了坚实的运输管道，运输触角四通八达。

快递业的飞速发展折射出我国蓬勃的经济活力以及企业和民众旺盛的消费能力。可以说，今天的中国很少有人或者企业完全没有接触过物流快递行业，没有购买使用过快递服务。因此，物流快递行业的信息安全问题对每一个人和每一家企业都至关重要。

[2] 数据来源：《新零售生态网络安全报告》

1.2 物流快递行业发展新趋势

1.2.1 信息技术的深度应用驱动物流快递行业智慧升级

在物流快递行业，软件定义物流成为物流快递行业的一大创新发展趋势。软件系统逐渐成为物流硬件的“大脑”，软件“大脑”通过联网实现不断进化与迭代创新，让物流自动化系统变得更加柔性和智能。自动化流水线、物流机器人、无人机等产品和系统，以及物联网、人工智能、机器学习、大数据、云计算、无人驾驶等技术得到越来越广泛的应用，既降低了劳动力成本，又提高了仓储和分拨的智能化和可视化能力，同时还催生出即时物流、新型社区末端网、前置仓网等新型服务模式，打通了物流“最后一公里”的末端配送网络，提升了客户的服务体验和行业运行效率。

1.2.2 快递企业纷纷加大海外拓展步伐

经济的全球化加剧了供应链体系的全球化，跨境电商因之而迅猛发展，国内大型快递企业也开始全球布局。例如，浙江菜鸟供应链管理有限公司（以下简称“菜鸟”）和物流合作伙伴搭建起可飞抵 40 余个国家和地区，共计 106 条航线的全球航空运输网络，服务覆盖 200 余个国家和地区。顺丰集团在新加坡、韩国、马来西亚、美国等十余个国家设立营业网点，至少开通了 14 条国际航线，物流服务覆盖了全球 200 余个国家和地区。可

以说，随着我国构建开放型经济的脚步不断加快，“一带一路”倡议稳步推进，国内物流快递行业将在不久的将来搭建起一张真正具有全球配送能力的跨境物流骨干网。

1.2.3 信息安全风险成为影响物流业健康发展的关键因素

近年来，我国信息泄露事件层出不穷，信息买卖日益猖獗，个人信息安全面临严峻挑战。中国消费者协会 2018 年个人信息安全调研数据显示，85.2%的受访者曾遭遇个人信息泄露问题，个人信息泄露的前三大途径分别是经营者未经个人同意收集个人信息，经营者或不法分子故意泄密、出售或者非法向他人提供用户个人信息，及网络服务系统存在漏洞导致个人信息泄露。信息安全问题同样是物流快递行业非常关注的问题。截至目前，快递服务出现过用户无法在线注销、安卓应用目标 SDK 版本设置过低等安全问题。近年来，快递行业迅速发展。2018 年全国快递服务企业业务量累计完成 507.1 亿件，预计 2019 将仍然保持两数增长。可以说，作为一个信息数据的海洋，快递信息的安全性至关重要。

二、物流快递行业面临复杂的信息安全形势

物流快递行业信息和数据安全一直是整个行业关注的焦点。近年来，从中央到地方各级政府陆续制定实施相关法律法规和政策标准，加强相关领域信息安全建设。

2.1 涉“快”信息安全问题多见

物流行业安全攻击频次高，攻击来源集中。根据菜鸟的数据，2018 年，菜鸟发现并拦截了针对物流行业的 4457 次有效攻击。分析发现，物流行业安全风险来源（境外攻击来源未统计在内）主要集中在长三角（如图 2 所示）：

图 2 物流信息安全风险来源分布情况

针对物流快递行业的网络攻击类型相对集中。2018 年下半年网警部门数据显示，网络攻击主要类型包括恶意扫描、网络攻击、僵尸木马蠕虫和拒绝服务攻击（如图 3 所示）。其中，恶意扫描在整体攻击发生频次上占比达 72%。实际形成的安全事

件共计 13 起，主要以挖矿木马、路由器后门利用和远程代码执行事件为主。

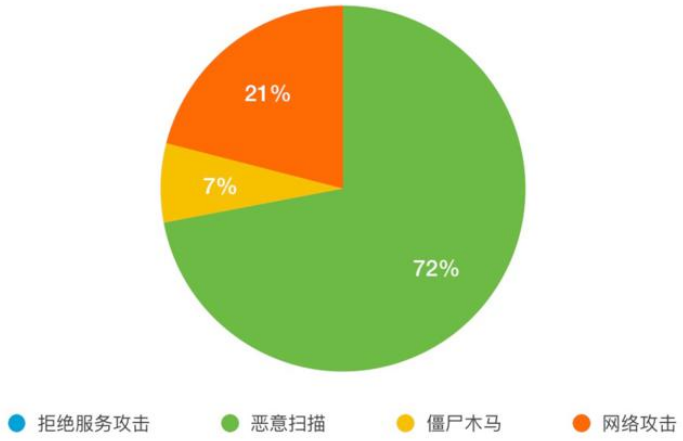

图 3 快递公司信息安全告警主要类型

物流快递行业业务链条长，信息安全管控面临更多挑战。物流快递业务链条较长，物流快递业务涉及多个线上线下相结合的复杂业务场景。这使得影响物流快递行业信息安全的因素多，风险管控复杂。

物流行业“黑灰产”活跃度不断上升。网络“黑灰产”是指通过电信诈骗、钓鱼网站、木马病毒、黑客勒索等方式，利用网络开展违法犯罪活动的行为。近年来，“网络黑灰产”规模已达千亿元，助长了网络“黄赌毒”、诈骗、敲诈勒索等多种网络犯罪滋生蔓延。根据 2018 年市场研究数据，物流行业“黑灰产”[3]活跃（如图 5 所示），给物流快递行业带来安全挑战。

[3] 《2018 网络黑灰产治理研究报告》。

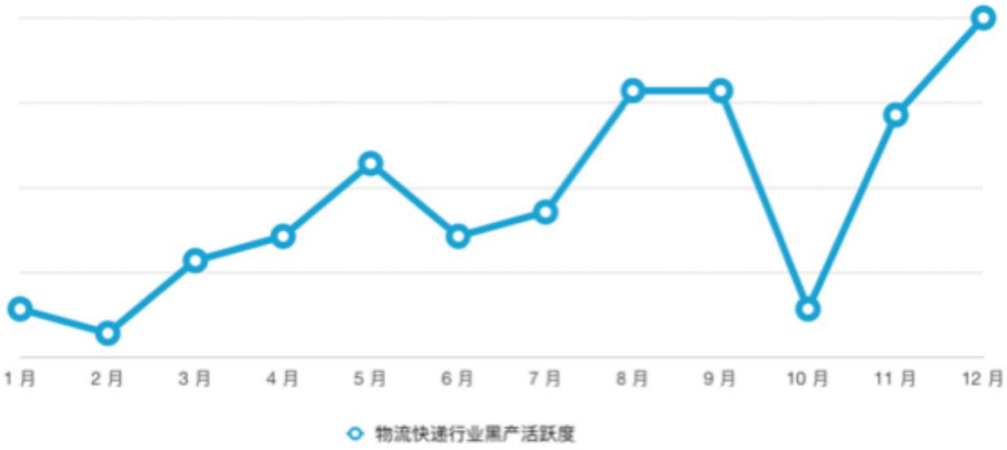

图 5 物流快递行业“黑灰产”活跃度

2.2 信息安全问题表现形式复杂化

从快递行业非法活动类型分布来看，网络诈骗类占比最多，其次是非法营销等其他违法活动，给消费者和企业造成经济损失。

首先，网络（含电信、即时通讯）诈骗成为主要信息安全风险。网络诈骗是指不法分子通过电话、网络和短信方式，编造虚假信息，设置骗局，对受害人实施远程、非接触式诈骗，诱使受害人给不法分子打款或转账的犯罪行为。2000 年以来，虚假信息诈骗犯罪，尤其是借助于手机、固定电话、网络等通信工具和现代的技术等实施的非接触式的诈骗犯罪，在我国迅速发展蔓延，给人民群众造成了很大的损失。

根据菜鸟监测数据，物流快递行业信息安全风险中，电信诈骗占比达到四分之一强。其中，因快递企业不规范使用即时通讯工具导致的安全风险问题上升，“黑灰产”不法分子潜入内部即

时通讯群组的情况也时有发生。如图 6 所示，即时通讯工具物流信息类诈骗呈现逐渐走高的趋势：

图 6 2018 年即时通讯类工具引发的诈骗

其次，“假包裹”欺诈层出。近期的“假包裹”欺诈主要表现为诈骗者用空包裹或者廉价物品装成到付快递寄给消费者，欺骗未购买该商品的消费者支付快递费。“假包裹”欺诈成为涉“快”犯罪的新形式。2018 年 2 月，上海市公安局青浦公安分局破获一起到付诈骗案。经查，犯罪嫌疑人招募工作人员，冒充知名品牌客服人员，通过微信散布免费赠送活动的虚假信息，诱使被害人支付 39 元运费，随后由闫某负责将包装好的伪劣产品使用货到付款的方式通过快递寄出，累计向全国各地发件 70 余万件。

2.3 法律规定与监管要求不断加强

网络安全关系到国家安全，受到党和国家高度重视。网络安全牵一发动全身，已成为信息时代国家安全的战略基石。正因为如此，习近平总书记在全国网络安全和信息化工作会议上强调，

没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。这一论述，把网络安全上升到国家安全层面，为加快我国网络安全能力建设指明了方向。2017年6月1日起施行的《中华人民共和国网络安全法》（以下简称《网络安全法》），是我国网络领域的基础性法律，明确强调了对个人信息的保护。《网络安全法》要求企业在发现网络产品、服务存在安全缺陷、漏洞等风险时，应当及时向用户告知并采取补救措施，否则企业负责人及相关安全责任人会受到不同程度的处罚。

信息安全监管机构及物流快递行业的主管部门加强物流快递行业信息安全治理。网信办、公安部、工信部及国家邮政局等部门要求快递企业应严守信息安全底线，并联合制定实施信息安全监管的措施，堵塞管理漏洞，严厉打击非法泄露、贩售用户寄递服务信息等各类违法犯罪行为，维护用户个人信息安全。2013年修订实施的《邮政行业安全监督管理办法》专设通信与信息安全章节，对保护用户信息安全作出具体规定。2016年出台的《网络安全法》要求网络运营者应当按照网络安全等级保护制度的要求，履行相应的安全保护义务。2017年，《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》正式出台，不仅进一步明确了侵犯公民个人信息罪的定罪量刑标准，而且规定“内鬼”作案加倍处罚。2018年正式实施的《快递暂行条例》设置保护个人信息安全单独条款，

对违法泄露用户信息的企业，情节严重的最高处 10 万元罚款，并可以责令停业整顿直至吊销其快递业务经营许可证。

依照这些法律法规，各地纷纷加强物流快递行业信息安全治理工作。以上海为例，2018 年，“三通一达”等 10 家快递企业的网站及重要信息系统（主要针对涉及公民个人信息的信息系统）进行了全面审查，共梳理出 52 个网站及重要信息系统。按照《网络安全法》要求，上海市对这些信息系统进行了网络安全等级保护定级和测评工作，其中 29 个系统为三级等保，23 个为二级等保。目前已有 40 个信息系统完成测评并取得证书，12 个信息系统已完成等保备案，正在整改中。关键信息基础设施和信息系统的信息安全等级保护工作切实加强了各快递企业信息系统防泄密、防渗透、防阻断的能力，降低了公民个人信息被泄漏的风险。

对快递行业信息泄漏等安全问题已出现司法实践，起到行业警醒作用。2018 年，湖北荆州中级人民法院审理宣判了深圳某快递公司员工及相关人员侵犯公民个人信息罪案件。涉案人员是该公司内部具有一定权限的工作人员，掌握着重要隐私内容，可在后台查看客户信息，先后泄露的公民个人信息达千万余条，涉及交易金额达 200 余万元。本案涉案人员分别被处以有期徒刑 10 个月到 3 年不等。此类案件给物流快递行业敲响了警钟，让全行业了解维护企业和公民信息安全收到法律保护，违法必究。

2.4 标准化成为信息安全治理的重要手段

网络安全标准作为网络安全保障体系建设的重要组成部分，在构建安全的网络空间、推动治理体系变革方面发挥着基础性、规范性、引领性作用。对于物流快递行业而言，网络安全标准也是其安全建设的重要基石。《网络安全法》规定，国家建立和完善网络安全标准体系，国家标准化主管部门和其他有关部门根据各自职责，组织制定网络安全管理及网络产品和服务的国家标准、行业标准。全国信息安全标准化技术委员会（以下简称“信安标委”或“TC260”，秘书处设在中国电子技术标准化研究院）在中央网信办和国家标准化管理委员会（以下简称“国标委”）的领导，以及有关网络安全主管部门的支持下，对网络安全国家标准进行统一技术归口和标准化工作。信安标委下设信息安全标准体系、涉密信息安全、密码、鉴别与授权、信息安全评估、信息安全管理、大数据安全等 7 个工作组，分别组织开展本领域标准化工作。

网络安全国家标准体系已初具规模。目前，全国信安标委已发布 268 项国家标准，在研 97 项标准制定项目，陆续制定实施了信息系统安全等级保护系列标准、产品安全测评、信息安全管理体系、信息安全风险评估、云计算服务安全、个人信息安全规范、大数据服务安全能力要求等标准。此外，关键信息基础设施保护、数据安全能力成熟度模型、数据出境安全评估、政务信息

共享安全、医疗信息安全等标准项目有些处于研制过程中，有些已经推进到报批稿阶段。

国家标准应用实践不断加强。近年来，越来越多的网络安全国家标准开展了广泛的应用实践。以大数据安全标准为例，2017年，信安标委在中央网信办、工信部、公安部和国标委的指导下，根据《网络安全法》及 GB/T 35273《信息安全技术 个人信息安全规范》有关内容，开展个人信息保护提升行动之隐私条款专项工作，对微信、淘宝网、京东商城等 10 款网络产品和服务的隐私政策进行评审。2018 年，信安标委继续对生活服务类、网络支付类等 5 类 30 款网络产品进行隐私政策评审，以提升相关企业个人信息保护水平。此外，国家标准《信息安全技术 数据安全能力成熟度模型》围绕数据生命周期，从组织建设、制度流程、技术工具和人员能力四个能力维度，给出了数据安全能力成熟度模型，该标准已在贵阳、成都、武汉三地及货车帮、伊利、南方电网、如家等多个行业近 100 家企业推广应用，2018 年信安标委也对互联网医疗、人工智能、物流、金融等领域十家企业开展了标准试点工作，为企业评价自身数据安全管理能力和水平提供了参考模型。

行业标准陆续出台。国家邮政局先后出台了《寄递服务用户个人信息保护指南》、《邮政业信息系统安全等级保护基本要求》等标准。这些国家和行业标准规范为物流快递企业及其信息化产品和服务供应商、信息安全服务机构等制定并实施隐私政策及个

人信息管理规范指明方向，成为相关企业和机构开展信息安全保护工作的技术指引。

三、快递企业信息安全风险防控实践

今天，快递企业面临着更加严格的法律规制和社会公众对保护信息安全日益高涨的呼声。从企业自身健康、安全、持续发展以及履行社会责任的角度出发，很多快递企业通过制定实施本企业信息安全风险防控制度和规范、在网络基础设施和信息系统建设进行更大投入、采用更高级安全防护技术等方式，系统性地推动风险防控工作，整体提升信息安全水平。

3.1 技术层面信息安全风险防控实践

保障信息安全需要技术先行。没有强有力的安全技术体系，就谈不上切实保障网络信息安全。据菜鸟统计，约 68%的行业安全风险与技术相关，如系统漏洞、账号/权限等。因此，采用先进的安全防护技术是保障物流快递信息安全的重中之重。

3.1.1 强化网络基础设施安全保障

网络基础设施在网络安全中占据着重要地位。对于网络基础设施进行攻击，往往会造成范围广、影响大、持续时间长的不良后果。例如，2017 年俄罗斯黑帽黑客“Rasputin”利用 SQL 注入漏洞获得了系统的访问权限，黑掉 60 多所大学和美国政府机构的系统，并从中窃取了大量的敏感信息。同年，洲际酒店旗下 12 家酒店餐厅及酒吧的支付系统被恶意软件入侵，顾客的信用卡支付信息被窃取。

安全、稳定的现代物流 IT 网络环境是快递企业业务稳定运行的前提，事关广大用户的切身利益。国内主流快递企业纷纷加大网络基础设施建设和维护投入，持续提升抗打击能力，降低安全风险隐患。以菜鸟为例，依靠阿里集团多年安全技术研究积累的成果和菜鸟物流云强大的分析能力,菜鸟为客户提供 DDoS 防护、主机入侵防护、漏洞检测和木马检测等一整套安全服务，从而为快递企业提供稳定、可靠、安全、合规的云计算基础设施服务。物流的云设施往往具备一般快递企业所不具备的专业安全风险防控能力，可以相对有效地控制风险，降低风险损害。

菜鸟物流云是基于云计算的物流基础信息服务平台,能提供安全稳定的云设施环境，为用户提供隐私保护通话服务、短信服务等安全类产品与服务。同时，菜鸟物流云形成通用解决方案和行业解决方案两大类解决方案，帮助快递企业有效抵挡外部攻击。

3.1.2 实施账号风控

账号安全是业务安全风险的重要入口，近年来，各大快递公司都在完善账号安全，例如中通快递为解决账号权限问题，利用 AI、大数据、机器学习等技术建设了统一身份认证和授权系统，增强了中通业务系统的安全性，其架构图如图 7 所示：

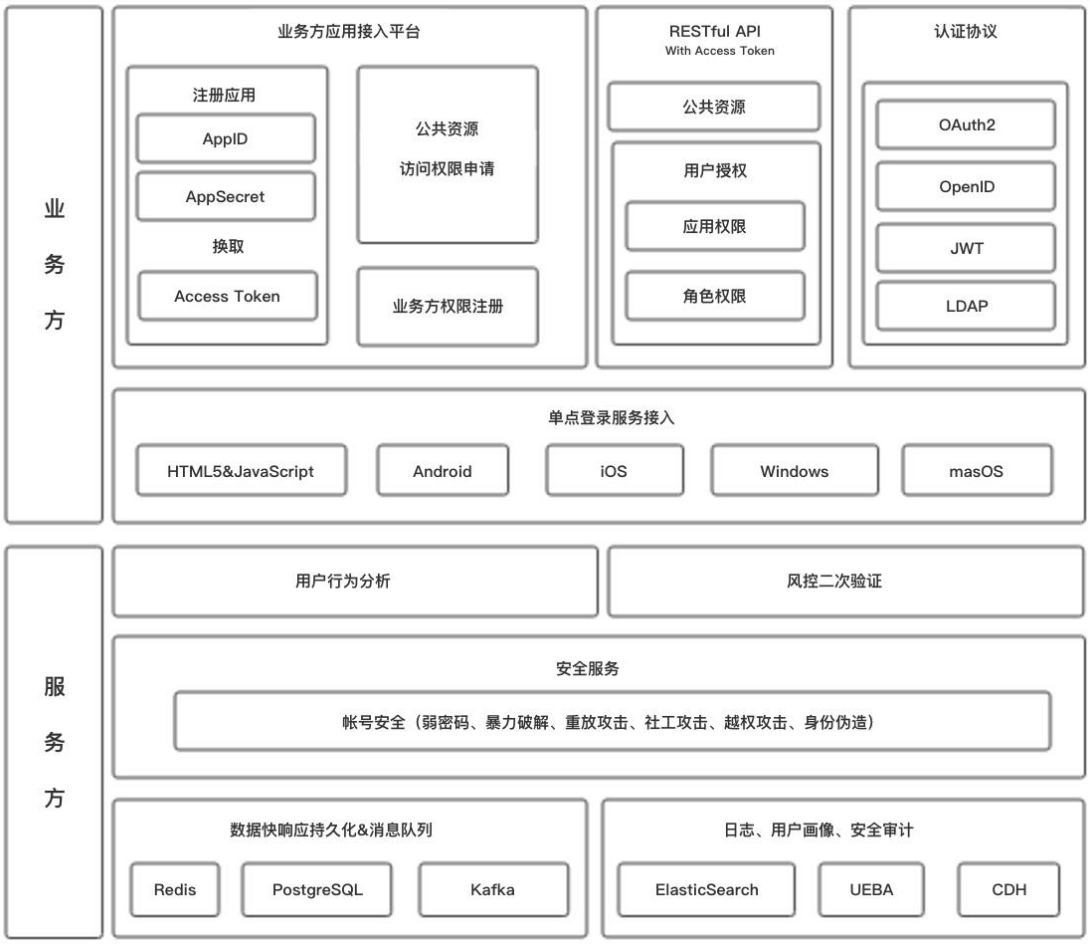

图 7 中通统一认证服务架构

同时，中通开发了快递查询软件——中通宝盒移动端 APP。通过这款软件，中通公司实现了对全网 30 万人员的实人验证以及系统帐号的闭环安全管理，在解决帐号管理难的同时也提高了操作的安全性和便捷性，保障了系统的安全准入。另外还实现了中通内部各个子系统认证以及多套帐号体系的互通，单个帐号可以在全网网点内自由切换和统一授权，满足了混合云架构下的自研系统及外购系统安全便捷接入的需求。

3.1.3 加强数据与隐私保护

当今社会，用户数据与隐私的保护越来越受到关注。菜鸟为物流快递行业用户提供高性能、低成本的数据与隐私安全服务。例如要求所有数据的使用都必须在隔离的网络安全域中使用，不同等级数据对使用的网络安全域有对应要求，不允许安全级别高的数据在低级别的网络安全域中使用。根据数据安全分级，对数据实施相应的保护策略。保证数据完整性，建立数据的灾难恢复和备份机制。

菜鸟利用 DSMM（数据安全能力成熟度模型）将数据安全管理经验标准化，其数据安全保障能力获得国内外权威机构的认可。菜鸟高分通过三级等保评定及历年复测评、具有 ISO27001 认证资质并通过历年年审、通过美国注册会计师协会（AICPA）SOC2 TYPE II 审计，获得 SOC2 TYPE II 和 SOC3 审计报告，成为国内首家通过 SOC2 审计的物流公司，其系统安全性、可用性和保密性处于国际先进水平。

3.1.4 构建物流安全管防控体系

以中国邮政速递物流为首的一些物流快递企业逐渐开始通过建立信息安全管防控体系来维护企业和用户信息安全。中邮速递依托生物识别技术、大数据和风险模型，建成了“E 盾”安全管防控平台。**管**，主要是管理邮件邮包中用户个人信息等敏感数据。在数据端实施加密脱敏，在应用端实施权限管控，并对生产

环节使用信息的内部人员应用手机认证、指纹识别等生物认证技术进行实人制认证。**防，**重点是防范黑灰产攻击盗取邮件邮包信息。通过结合业务场景、流程、账号属性设计防御阈值，对超出工作正常需要的异常行为主动防御，自动注销工号并触发系统短信告警，自动通知专职安全管理员开展调查。**控，**重点是控制风险行为。依托大数据技术对海量日志数据进行智能分析，结合账号登录异常、账号查询量异动、账号越权访问、服务流量异常等风险模型，实施风险识别预警和主动安全防御。平台建成以来，已对数起可疑行为进行主动拦截和预警，结合现场逐一复查，强化了用户数据安全意识，有效遏制了黑灰产业渗透窃取信息行为。

3.2 其他层面信息安全风险防控实践

物流快递行业信息安全治理需要内外共治、技术管理并行。很多公司都开展了很好的尝试。

一是建立并实施企业信息安全管理制度规范，加强企业内部信息安全管理。以菜鸟为例，从机制保障、人员保障和数据使用安全保障等方面加强数据安全保护。例如指定事业部、业务部门负责人为各自业务范围内的数据安全第一责任人。**在**公司内部开展各类培训对员工进行全方位的宣传教育。定期对数据可行性进行评估，对不可用或不再用数据及时销毁。严格遵循数据最少够用原则。数据开放过程中必须明确第三方使用数据的法律责任，且第三方使用数据的环境必须满足数据的安全性保护要求等等。

二搭建物流安全服务平台，优化安全服务环境。为提升各家物流公司信息安全水平，提供给消费者及企业一个更加安全的网络环境，上海市青浦公安部门联合菜鸟和主要物流企业发布了“物流安全服务平台”，目前申通、圆通、中通、韵达等公司均已接入这一平台。该服务平台充分借鉴互联网企业安全保护良好实践，整合行业安全和相关机构等资源，进行信息安全风险预警，在物流企业进行风险监测、识别、评价和管控工作中发挥较大作用。

三是广泛联系企业，组建安全联盟，搭建物流快递信息安全“生态圈”。菜鸟发起成立“菜鸟物流快递行业安全联盟”，与物流快递业同行（中国邮政、中通、韵达、圆通、申通、百世、德邦、苏宁、日日顺物流、优速、安能等）在信息安全、网络安全、黑灰产对抗方面加强合作与交流，协助相关机构防范打击阻碍行业健康发展、侵害用户合法权益的网络“黑灰产”及各类恶意攻击。

四是创新服务模式，提升用户信息保护水平。从 2018 年开始，菜鸟平台，以及京东、顺丰、中通等物流快递公司开始普及使用隐私面单，对面单上的消费者信息包括姓名、电话等进行技术处理，不直接显示在快递面单上，并且只允许派件员查看。对用户手机号码加密处理，派件员也只能通过 APP 直接进行拨打，

无法看到号码等。这些措施在一定程度上提升了用户隐私保护力度。

四、全局入手加快提升物流快递行业信息安全水平

物流快递行业的繁荣，与“新零售”的迅速发展密切相关，在物流快递行业帮助“新零售”走完“最后一公里”的同时，也使得物流快递行业信息安全治理变得极其重要。物流快递行业的信息安全治理需要政府、行业组织、企业、公众等各利益相关方共同参与、共同投入。为构建安全、便捷、高效的安全环境，本报告尝试提出以下建议：

4.1 加强物流快递安全相关法律制度建设

首先，目前与物流快递安全相关的法律主要有《网络安全法》及相关配套法律法规、《中华人民共和国邮政法》和《快递暂行条例》等物流快递行业法律法规。这些法律法规仍存在内容零散、针对性不足等问题。因此，建议围绕《网络安全法》等通用法律法规要求，结合物流快递行业的特点，制定物流快递行业的个人信息保护、数据安全等相关政策法规。此外，加强《刑法》、《民法》、《消费者权益保护法》等相关法律法规中对于泄露信息，侵犯消费者权益、危害公共利益和社会秩序的个人和组织的惩罚力度。

其次，加强跨部门、跨区域协作配合，加强物流快递行业信息安全监管与执法力度。对于出售、非法提供和窃取、获取用户个人信息等违法犯罪行为，坚持零容忍，依法严厉打击。寄递企业及从业人员一旦发生出售、非法提供和窃取、获取用户个人信

息等违法行为，邮政管理部门将根据违法行为的情节及危害后果，对涉事企业作出罚款、停业整顿、吊销经营许可等行政处罚，构成犯罪的将依法移送司法机关。

4.2 引导企业提高信息安全保护力度

首先，很多快递企业在向以数字化、智能化为核心的智慧物流转变过程中，在建设 IT 系统与采用自动化设备方面投入巨额资金，而在信息安全建设方面投入不足，部分物流快递企业甚至没有专职安全人员，也尚未制定企业信息安全保护制度规范。因此，相关政府部门、行业组织、媒体应切实加强对物流快递行业信息安全问题严重性、信息安全治理重要性的宣传，提高企业的安全防护意识。物流快递企业管理人员应加强对企业内部人员的信息安全培训，在日常工作中树立起安全是现代化企业的生命线的观念。

其次，鼓励物联网、传感器、大数据、云计算、人工智能等新型信息技术，以及网络入侵检测、入侵防御、安全隔离、数据管理等信息安全技术的研发和应用。引导快递企业加强与信息安全服务提供商的合作，共同构建全生命周期的纵深安全防御体系，在提高企业经营效率的同时全面提升信息安全保护水平。

再次，加强信息安全标准化建设。技术标准作为固化技术创新成果的重要载体，在推进技术创新中发挥着重要作用。应鼓励

和引导重点快递企业、互联网企业、信息安全企业积极参与国家和行业标准的制修订，逐步建立系统、科学的物流快递信息安全标准体系。

最后，鼓励企业开展服务模式创新，提升信息安全保护水平。在全国范围内大力推广使用电子面单，指导寄递企业采取身份掩护、权限管理、信息加密、建立线上线下投诉举报制度等多种措施，强化对寄递用户个人信息保护。

4.3 整合多方力量共筑行业安全生态

首先，充分发挥产业联盟和行业组织的作用，加强物流快递行业内部在信息安全保护、网络空间治理、黑灰产对抗等方面的交流与合作。通过交流与合作，形成物流快递企业、互联网企业、信息安全服务提供商互相借鉴学习的机制，从而完善企业的安全管理手段，提升安全防护技术能力。

其次，加强快递企业、互联网企业、信息安全服务商与网信办、工信部、公安机关、邮政管理部门等主管部门的联动机制，在共同应对重大信息安全事件、对抗网络黑灰产等方面深度合作、形成合力，做到群防联防，共建安全、和谐的物流生态环境。

再次，行业协会是政府和企业之间的桥梁和纽带，对维护行业发展利益、营造健康有序的发展环境起到重要作用，同时也应承担起相应的责任。邮政快递领域行业协会应根据组织章程，制定并实施行业信息安全行为规范，加强行业自律。组织开展信息

安全咨询和培训，提高全行业对信息安全风险及信息安全治理的重视，指导会员单位加强信息安全保护。

最后，依托网络安全相关国家法律法规和标准规范，大力发展信息安全服务业，构建网络安全社会化服务体系。支持专业、权威的网络安全认证、检测和风险评估服务机构不断提高技术水平和提高业务素质，为物流快递企业提供风险评估、安全测评、产品和服务认证，以及解决方案服务。