2026年3月23日 星期一
本版主编：于 南 责 编：张 博 制 作：李 波
证券日报

金融深一度

AI智能体加速落地 商业保险迎补位时刻

本报记者 冷翠华

近日，国家互联网应急中心等部门接连发布AI相关风险提示，引发市场广泛关注。这一现象也折射出，随着AI加速融入人们的工作与生活，网络安全风险的形态也在持续演变——从传统的信息系统漏洞，逐渐向高权限自动化执行带来的新型安全隐患延伸。

当AI智能体具备调用系统、读取数据、连接外部工具的能力时，安全防护的复杂性也随之增加。一旦发生误操作、越权执行或被恶意利用，可能会对企业和个人造成不利影响。因此，对于蓬勃发展的AI产业而言，网络安全保险不仅是事后补偿的工具，更是稳定创新预期、护航技术商业化落地的重要配套机制。

多位受访业内人士向记者表示，随着AI技术的广泛应用，网络攻击正呈现智能化、隐蔽化特征，单一节点的安全隐患可能引发更广泛的连锁反应。在统筹发展与安全的背景下，网络安全保险迎来了新的发展空间。然而，供需错配、行业标准有待完善等现实挑战依然存在。如何让商业保险更好“补位”，已成为护航AI产业高质量发展的必答题。

AI智能体带来新型风险

AI智能体的出现可能让网络安全风险进一步升级。近日，国家互联网应急中心发布风险提示称，AI智能体面临提示词注入、误操作、插件投毒和安全漏洞等多重风险。例如，攻击者可在网页中植入隐藏指令，诱导智能体泄露密钥或敏感数据；恶意插件还可能窃取密钥、植入木马，导致终端被远程控制。

事实上，类似风险已在企业级AI助手和AI代理场景中暴露。微软曾公开提示，间接提示词注入已成为AI系统常见攻击方式，攻击者可借助邮件、网页、文档中的恶意内容，诱导系统泄露信息或执行非预期操作。

这些案例表明，一旦AI智能体被赋予较高系统权限，其误操作、越权执行或被恶意利用，便可能迅速演变为真实的业务与安全事故。

达信（中国）保险经纪有限公司（以下简称“达信中国”）财务及专业责任风险负责人常寿康对《证券日报》记者表示，AI技术的发展非但没有简化网络安全防护，反而扩大了攻击面、加剧了攻防不对称。“攻击者可利用AI生成自动化攻击工具和深度伪造内容，降低攻击门槛；防御方需要投入更多资源进行实时监测和响应，传统防御手段已难以应对AI赋能的新型攻击。”

常寿康进一步表示，未来网络风险将出现三大趋势：一是智能化，AI让攻击更隐蔽、更快速；二是扩大化，攻击面从传统IT系统延伸至物联网、工业控制系统，网络攻击可能转化为物理世界的生产安全事故；三是系统化，行业高度互联导致单一节点风险易通过供应链传导，引发大规模系统性损失。

业内人士普遍表示，针对AI智能体带来的新型风险，目前相应的保险产品还较少，要防范并转移新型风险，还需要险企、网络安全企业等加强融合创新。

网络安全保险需求增长

在网络安全风险持续升级的背景下，网络安全保险市场也逐渐升温。作为网络安全与金融服务的创新融合产物，网络安全保险通过经济补偿、风险管控等方式，为企业和个人提供财务韧性支撑，已成为数字经济时代风险管理的重要工具。

政策的持续完善，为网络安全保险的发展提供了强大支撑。2023年，工业和信息化部与国家金融监督管理总局联合印发《关于促进网络安全保险规范健康发展的意见》，明确了“技术+保险”的融合发展路径。此后，第一批次、第二批次网络安全保险服务试点相继启动。2026年3月份，科技部等四部门联合发布意见，提出推动网络安全保险创新应用，持续开展网络安全保险服务试点，发布网络安全保险服务典型方案目录，扩大保险应用范围。

在政策的引导下，企业投保需求持续释放。达信中国网络安全风险负责人韩祎介绍，近年来，随着中国企业数字化进程加速及“走出去”步伐加快，网络安全保险市场稳步增长，保费规模持续扩大。她表示，市场驱动力主要来自四个方面：一是监管与合同要求，二是供应链合作需求，三是第三方索赔风险，四是企业风险管理意识提升，管理层对网络安全事件的重视程度不断提高。

从市场供给来看，网络安全保险产品体系不断丰富。主流产品主要围绕第一方损失保障和第三方责任保障两大核心构建，前者主要覆盖企业自身的直接经济损失，后者则覆盖企业对第三方的法律赔偿责任。

从公开信息看，严格意义上直接以“AI网络安全保险”命名的成熟标准化产品仍较少，市场更多以“AI责任保险+网络安全扩展保障”方式切入。保险公司与保险经纪机构正持续探索服务新模式。记者了解到，中国平安财产保险股份有限公司（以下简称“平安产险”）近3年来已落地保单超1500张，保费规模超7500万元，提供超100亿元保额的网络安全风险保障。达信中国则依托全球化资源，提供从投保前风险评估、投保中方案设计到投保后理赔管理的全流程服务。

发展瓶颈亟待突破

尽管网络安全保险市场持续升温，但目前仍面临供需错配、标准缺乏等问题。受访人士认为，推动网络安全保险市场健康发展，护航技术创新与商业化落地，更好守护数字经济时代安全，还需多方协力。

北京排排网保险代理有限公司总经理杨帆对《证券日报》记者表示，一方面，企业端对风险的认知不足，往往重合规、轻保障，需求尚未完全释放；另一方面，供给端因缺乏统一的风险评估标准和历史损失数据支撑，导致产品定价难、核保难且同质化严重，同时保前风险量化与保后理赔定损的技术服务链条尚未打通，制约了市场发展。

平安产险相关负责人对《证券日报》记者表示，与车险和普通财产险相比，网络安全的保费和理赔数据量远远不足，再加上网络攻击手段不断迭代更新，对保险公司提出较大挑战。此外，网络安全保险生态体系有待完善。各方主体的分工协作有待更多实践，当前保险公司的重点还聚焦在保险产品本身，未形成成熟的服务模式。

此外，新业态、新技术不断推高风险复杂度，但相应产品和风险转移方案仍显薄弱。韩祎表示，目前市场上的网络安全保险产品主要针对传统网络安全风险设计，对于AI智能体带来的新型风险，如AI系统本身成为新的攻击目标，尚没有完善的保障机制。对于个人和“一人公司”而言，相关保障也比较缺乏。

为更好地推动网络安全保险落地，共建网络安全保险良性生态，平安产险相关负责人建议，加大企业引导力度，构筑“强制、补贴、鼓励”三位一体的政策体系，切实提高企业投保意愿。同时，推动网络安全保险行业标准建设，加快可量化的网络安全风险评估体系、事故定责定损标准建立。此外，完善网络安全保险产品体系和服务模式，推动产品创新。

杨帆则建议积极探索“保险+再保险”的风险分散机制，引入参数化保险等创新形态，推动网络安全保险与网络安全服务产业深度融合，提升企业应对网络突发事件的韧性与恢复能力。

整体而言，随着AI技术的持续渗透和数字经济的深入发展，网络安全风险将更加复杂多样，网络安全保险作为风险转移的核心工具，迎来了前所未有的发展机遇。不过，供需错位、生态融合度较差等问题仍制约着市场发展，尚需多方协同、精准发力。唯有推动产品创新、体系完善，才能让网络安全保险真正发挥“安全屏障”作用，为数字经济高质量发展筑牢安全根基。

制造业转型升级 特色智能体迎发展机遇

本报记者 郭冀川

近期，工业和信息化部召开干部大会，会议提出，开展制造业数字化转型行动，深入实施“人工智能+制造”行动，培育一批特色智能体。这些举措将深度拓展智能体在制造业领域的应用范畴，使其成为推动制造业转型升级的核心驱动力，引领行业迈向全新发展高度。

今年1月份，工业和信息化部等八部门联合发布的《“人工智能+制造”专项行动实施意见》提出，到2027年，我国人工智能关键核心技术实现安全可靠供给，产业规模和赋能水平稳居世界前列。同时，业内普遍预计，2026年智能体将步入快速发展的黄金时期。

当下，智能体不仅广泛应用在智能制造工厂，还在众多领域崭露头角。在医疗领域，智能问诊系统已经实现商用，智能体拥有规模庞大且内容丰富的医学知识库，当患者前来就诊时，智能体能够迅速对患者提供的症状、病史等信息展开全面剖析，并与知识库中的数据进行细致比对，协助医生进行疾病诊断。

在近期举行的2026中关村论坛年会线下走访活动中，《证券日报》记者来到北京罗森博特科技有限公司，该公司创始人及董事长王豫向记者介绍，公司研发的智能化骨科机器人以数智化手段“复刻”临床专家经验，将专家的经验完美传承。在现场模拟演示中，机器人具备精准定位、安全置入螺钉等功能，真正实现了精准、安全的骨折微创治疗。

在交通领域，自动驾驶系统依托感知、决策、控制一体化能力，以前装量产级车规设计与“视觉为主+固态激光雷达”融合感知为核心，打造交通智能体，实现复杂场景下稳定可靠的环境感知、路径规划与动态决策，为自动驾驶车辆提供安全高效的自主行驶能力。

蘑菇车联信息科技有限公司总裁付强在接受《证券日报》记者采访时表示，蘑菇车联自主研发的自动驾驶系统以数据和AI为驱动赋能交通场景，以自动驾驶巴士为载体，推动“AI+公共交通”深度融合，实现城市公共服务智能升级，将科技创新转化为稳定、安全的出行服务生产力。通过海量真实路况数据训练，自动驾驶车辆在复杂城市场景中能够迅速生成最优驾驶决策，完成从“规则驱动”“数据驱动”到“认知驱动”的跨越。

在智能体快速发展的进程中，安全问题也成为业内关注的焦点，其关乎智能体的应用落地成效。《“人工智能+制造”专项行动实施意见》明确提出，支持模型训练和推理方法创新，开发适应制造业实时性、可靠性、安全性特点的高性能算法模型。这为智能体的安全发展指明了方向。

中国移动通信联合会教育与科学技术研究院执行院长陈晓华在接受《证券日报》记者采访时表示，为确保智能体的安全，企业可综合运用多种技术构建多层次防护体系，如通过分布式账本和哈希链技术，确保智能体运行数据、决策记录的完整性与可追溯性，防止数据被恶意篡改或伪造。

为抵御量子计算攻击，陈晓华表示，企业可部署抗量子攻击的加密算法，保障长期安全性。此外，通过智能安全监测系统，实时监测智能体的运行状态，及时发现并预警潜在的安全威胁，时刻守护智能体的安全。

中关村物联网产业联盟副秘书长袁帅对记者表示，随着“人工智能+制造”行动的深入推进，智能体应用愈发广泛，企业也需为智能体的安全运行提供制度保障，要严格依照制度和规范操作，加强对智能体的安全管理与维护。例如，定期对智能体进行安全评估，及时发现并整改存在的安全问题，这对企业的人才团队建设和技术实力提出了更高要求。

绿电产业新型商业模式有望涌现

本报记者 吴奕萱

东方财富Choice数据显示，近一个月来，A股绿色电力板块市值整体上行。

受访专家普遍认为，我国绿电产业正逐渐迈入成熟发展阶段。未来，绿电与算力、储能、工业消费的融合会进一步加深，行业将从单纯比拼装机规模，转向更注重消纳利用、商业模式创新和产业链协同。

有望再迎黄金期

绿电是指利用太阳能、风能、水能、生物质能等可再生能源生产的电力，具有低碳清洁、可持续的特点。

近年来，在“双碳”目标的指引下，我国绿电产业规模实现了跃升式发展。国家能源局数据显示，2025年，全国可再生能源发电新增装机4.52亿千瓦，同比增长21%，占全国电力新增装机的83%。

业内人士认为，随着AI时代的到来，我国绿电产业有望迎来新一轮发展黄金期。华创证券发布的研报显示，伴随AI驱动的算力需求的爆发式增长，电力成本在数据中心总运营支出中的比重或将持续攀升，绿电展现出的低电价优势为数据中心降本提供了有效途径。

“算力中心既是AI核心设施，也是耗电大户。”眺远咨询董事长兼CEO高承远在接受《证券日报》记者采访时表示，“AI的尽头是电力，而电力的尽头是绿电。AI算力的爆发将推动绿电产业从传统公用事业向数字能源基础设施跃迁。”

上市公司加强布局

绿电产业发展壮大的同时，多元化的新需求、新赛道也应运而生。为抢抓发展机遇，绿电产业链上市公司纷纷加紧布局，推动绿电直连、算电协同、源网荷储一体化、交能融合等新型商业模式加速落地。

绿电直连方面，今年1月份，哈尔滨九洲集团股份有限公司在投资者互动平台上表示，公司已经建设了个别绿电直连项目，还有些绿电直连项目正在申报中。公司完全掌握风光生物质等新能源绿电直连相关技术和解决方案，会在项目收益和风险可控的条件下，加大探索绿电直连项目的开发和投入。

算电协同方面，2025年，浙江伟明环保股份有限公司分别与温州市龙湾区人民政府、中国移动温州分公司签署《人工智能产业发展战略合作框架协议》《战略合作协议》，旨在探索垃圾焚烧发电项目协同建设智算中心的商业模式，打造具有示范意义的“绿电+算力”标杆项目。

“融合型新赛道的涌现既能提升绿电消纳与利用效率，也催生了更可持续的商业模式，传递出能源转型向纵深发展的积极信号。”高承远表示。

有机构人士在接受《证券日报》记者采访时表示，上市公司积极布局产业新赛道，一方面，旨在抓住新需求为上市公司提供新的利润增长点；另一方面，上市公司凭借资本实力与资源整合能力，能够迅速将前沿技术转化为可落地的商业项目，这有利于绿电产业的高质量发展。

金价大幅震荡短期承压 中长期上行逻辑仍存？

本报记者 张梦逸

近期，黄金价格大幅震荡，引发市场关注。

从国际金价来看，截至北京时间3月21日收盘，COMEX黄金跌破4500美元/盎司关口，报4492美元/盎司，当日跌幅为2.47%，周内累计跌幅超10%。国内金价同步下行，截至3月20日收盘，沪金期货主力合约报1016.12元/克，下跌1.22%。

受金价下行影响，国内珠宝品牌普遍下调金饰价格。3月22日，周大福、周生生、六福珠宝等品牌足金饰品克价均下调至1400元/克以下。

针对本轮金价下跌，陕西巨丰投资资讯有限责任公司高级投资顾问于晓明向《证券日报》记者表示，主要原因是美联储释放强烈鹰派信号，市场降息预期显著降温，美元与美债收益率走高对无息黄金构成压制。

北京时间3月19日，美联储宣布将联邦基金利率目标区间维持在3.5%至3.75%之间不变。这是今年以来美联储连续第二次维持利率不变。

中国邮政储蓄银行研究员娄飞鹏认为，除受美联储鹰派信号影响外，地缘冲突推高油价，加剧通胀担忧，避险资金转投美元、原油，也减少了对黄金投资的需求。另外，前期高位获利盘获利了结，多重利空因素导致黄金价格下调。

“短期金价大概率震荡承压，中期若美联储启动降息，实际利率下行，叠加央行购金支撑、地缘冲突风险持续，金价有望重启涨势。”谈及黄金价格后续走势，娄飞鹏表示，从长期来看，受供需缺口等因素影响，黄金价格大概率仍呈现上涨趋势。

东方金诚研究发展部高级副总监瞿瑞认为，后续金价将呈现“短期承压、中长期向好”的走势。短期内，原油价格高企将令美联储高利率维持更久、美元强势，继续压制金价。中长期来看，随着油价上涨效应递减、通胀逐步回落，美联储降息周期虽推迟但不会缺席，叠加各国央行购金需求稳定、美元信用弱化共振，金价有望震荡回升。

“短期建议投资者保持观望，规避抄底风险，等待支撑位确认。中长期则应重点关注美联储降息窗口及地缘局势演变等核心催化因素。”瞿瑞表示。

黄金产业链上市公司 业绩分化或加剧

本报记者 李 静

近段时间，黄金产业链上市公司陆续发布2025年业绩情况。在2025年金价持续突破、高位运行的背景下，相关上市公司业绩普遍走高，但也有部分公司业绩下滑。业内人士认为，随着黄金价格震荡，产业链上市公司业绩分化或加剧。

具体来看，处于产业链上游的黄金矿企成为金价上涨的最大受益者。紫金矿业集团股份有限公司发布的2025年度业绩公告显示，公司全年实现营业收入3490.79亿元，同比增长14.96%；实现归母净利润517.77亿元，同比大增61.55%。

赤峰吉隆黄金矿业股份有限公司同样业绩喜人，2025年度实现营业收入126.39亿元，同比增长40.03%；实现归母净利润30.82亿元，同比增长74.70%。

山东黄金矿业股份有限公司预计2025年度实现归母净利润46亿元至49亿元，同比增长56%至66%；实现归母扣非净利润48亿元至51亿元，同比增长60%至71%。

万联证券投资顾问屈放在接受《证券日报》记者采访时表示，上游黄金矿企具备典型的资源属性，开采成本相对刚性，金价高位运行直接转化为毛利率与净利润的大幅提升，叠加头部企业持续扩产增储，实现量价齐升的高增长格局。行业集中度进一步提升，具备资源储备与成本优势的龙头企业，盈利弹性与抗风险能力显著领先。

与上游矿企形成鲜明对比的是，下游黄金珠宝零售商业绩分化明显。传统金饰龙头老凤祥股份有限公司发布的业绩快报显示，2025年公司实现营收528.23亿元，同比减少6.99%；归母净利润17.55亿元，同比下滑9.99%。此外，沈阳萃华金银珠宝股份有限公司、浙江明牌珠宝股份有限公司预计2025年业绩出现同比下滑或亏损。

然而，部分注重品牌溢价和产品差异化的企业业绩普遍增长。广东潮宏基实业股份有限公司预计2025年实现净利润4.36亿元至5.33亿元，同比增长125%至175%。老铺黄金股份有限公司预计2025年实现销售业绩约310亿元至320亿元，同比增长约216%至227%；经调整净利润约50亿元至51亿元，同比增长233%至240%。

屈放进一步分析称，下游零售行业受高金价冲击分化明显，传统金饰企业业绩承压，品牌化、差异化布局的企业则逆势突围，行业正加速向精品化、品牌化转型。

值得关注的是，近期，国际金价剧烈震荡。前海开源基金首席经济学家杨德龙对《证券日报》记者表示，本轮地缘冲突引发市场连锁反应，通胀预期上行迫使美联储推迟降息，叠加前期金价大幅上涨积累的获利盘集中了结，导致短期价格回调。

展望后市，机构对黄金长期走势仍持乐观态度。申银万国期货认为，市场对美国财政可持续性担忧仍在加剧，叠加全球政治经济秩序重构、全球央行储备资产多元化，黄金有望保持长期上行趋势。