

# 1—7月我国软件业务收入同比增长21.4%

## 工信部运行监测协调局

1—7月，我国软件和信息技术服务业（以下简称软件业）发展态势平稳，业务收入持续快速增长，软件出口和利润总额增速放缓，从业人数稳步增加。

## 总体运行情况

软件业务收入保持快速增长。1—7月，我国软件业完成软件业务收入51441亿元，同比增长21.4%，增速比上年回落1.8个百分点，近两年复合增长率为14.8%，较上半年提高0.1个百分点。

利润总额增长持续放缓。1—7月，全行业实现利润总额5838亿元，同比增长12.3%，比上年回落1.3个百分点，近两年复合增长率为8.8%。

软件出口稳中趋缓。1—7月，软件业实现出口290亿美元，同比增长10.9%，近两年复合增长率为6.6%。其中，外包服务出口81.8亿美元，同比增长17.9%；嵌入式系统软件出口110亿美元，同比增长3.6%。

从业人数规模小幅扩大，工资总额增长平稳。1—7月，我国软件业从业平均人数767万人，同比增长6.4%，规模比上年增加14万人；从业人员工资总额同比增长11.6%，增速与上半年持平，近两年复合增长率为8.0%，较上半年提高1.6个百分点。

## 分领域运行情况

软件产品收入增速稳中有落。1—7月，软件产品实现收入13402亿元，同比增长17.5%，比上年回落2.6个百分点，占全行业收入的比重为26.1%。智能制造、工业互联网等政策利好持续释放，推动工业软件产品收入完成1273亿元，同比增长17.0%，占软件产品收入比重为9.5%，占比较去年同期提高0.5个百分点。

信息技术服务收入平稳较快增长。1—7月，信息技术服务实现收入32744亿元，同比增长24.6%，比上年回落1.4个百分点，在全行业收入中占比为63.6%。其中，云计算、大数据服务共实现收入4298亿元，同比增长22.8%，占信息技术服务收入的13.1%；电子商务平台技术服务收入4626亿元，同比增长29.3%；集成电路设计收入1289亿元，同比增长31.4%。

信息安全行业稳步发展。政策的执行落地驱动数据安全及隐私保护的产品和服务需求升级扩容，信息安全行业迎来重要发展机遇。1—7月，信息安全产品和服务共实现收入883亿元，同比增长21.9%，高出全行业平均水平0.5个百分点。

嵌入式系统软件收入增速小幅回落。1—7月，嵌入式系统软件实现收入4413亿元，同比增长11.4%，比上年回落1.4个百分点。

## 分地区运行情况

东部地区软件业收入平稳较快增长，中部地区增长明显放缓。1—7月，东部地区完成软件业务收入41304亿元，同比增长21.8%，比上年回落1.9个百分点，高出全国平均水平0.4个百分点。中部地区完成软

件业务收入2341亿元，同比增长21.8%，比上年回落3.7个百分点。西部地区完成软件业务收入6286亿元，同比增长20.1%，比上年回落1个百分点。东北地区完成软件业务收入1511亿元，同比增长15.3%，比上年回落0.6个百分点。四个地区软件业务收入在全国总收入中的占比分别为80.3%、4.6%、

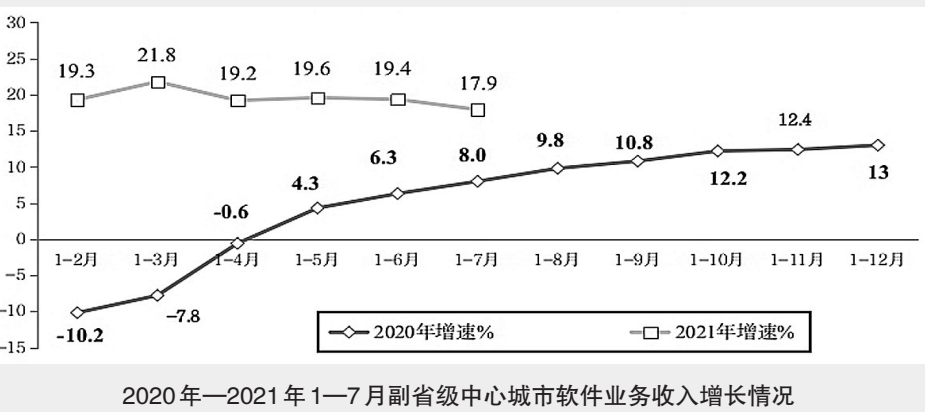
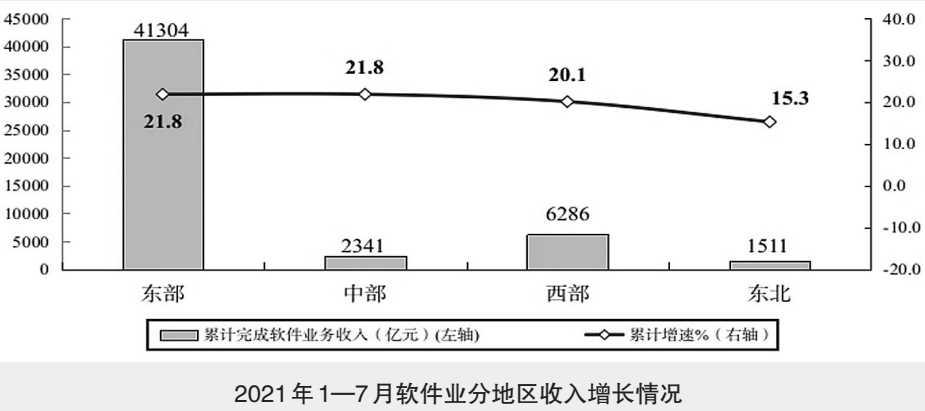
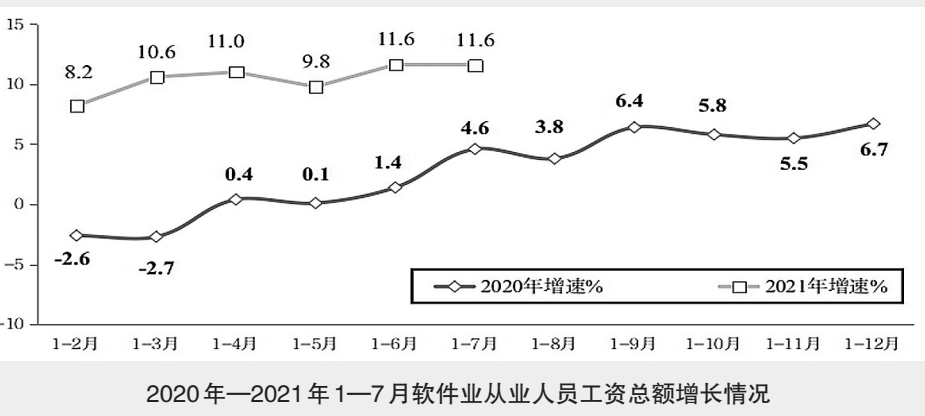
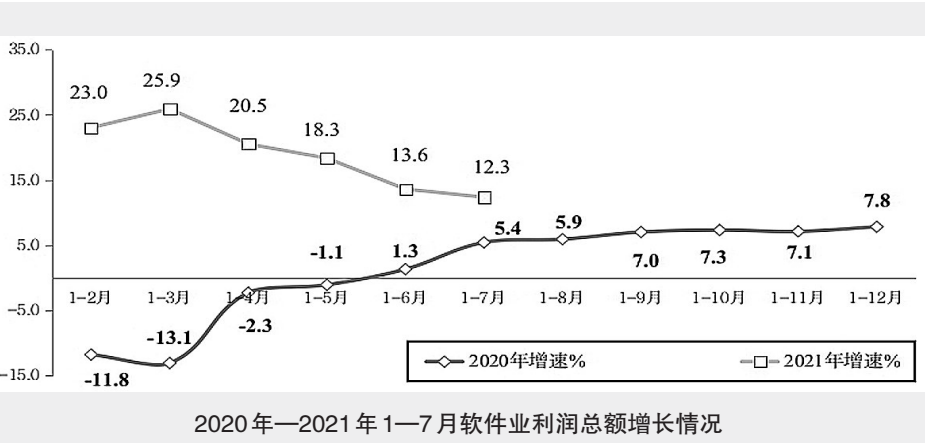
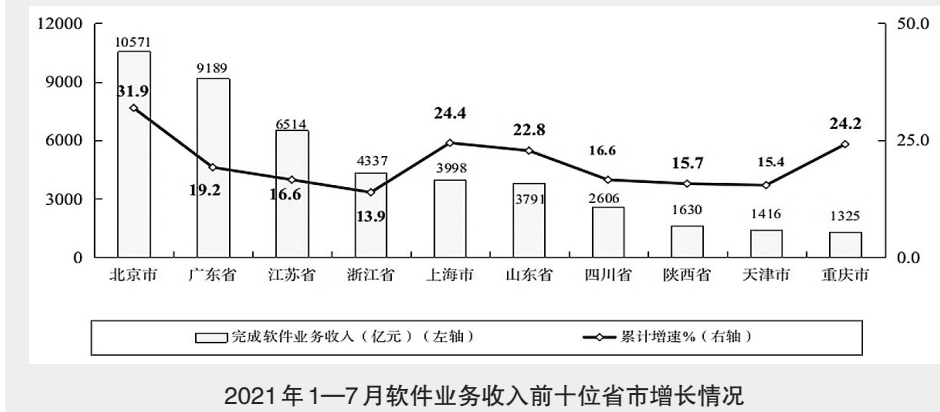
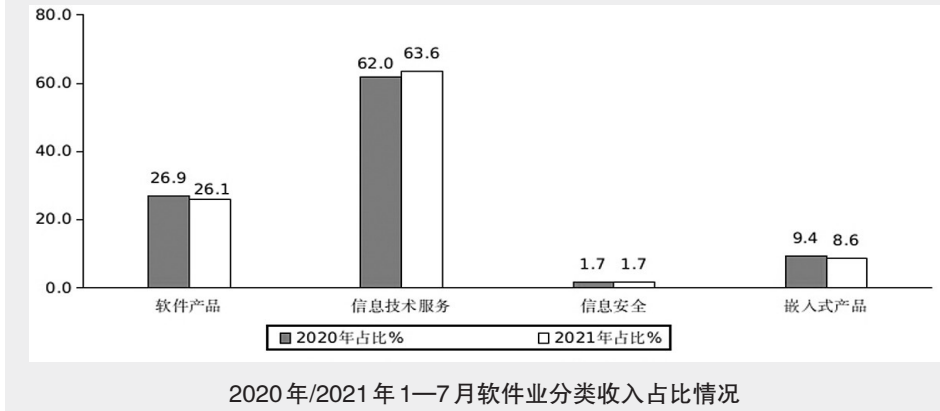
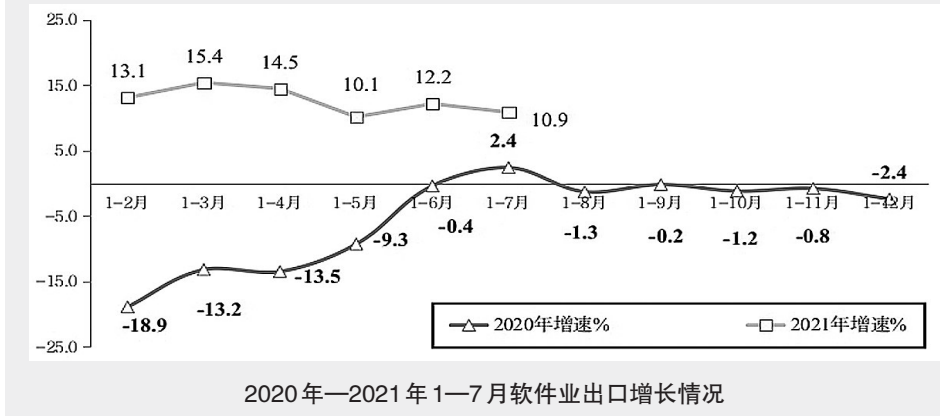
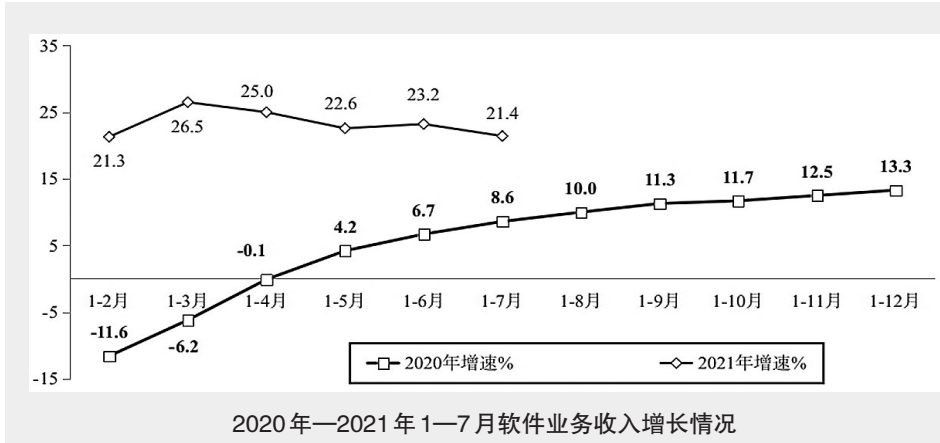
12.2%和2.9%。

主要软件大省保持两位数增长。1—7月，软件业务收入居前6名的省份中，北京、广东、江苏、浙江、上海和山东软件收入分别为10571亿元、9189亿元、6514亿元、4337亿元、3998亿元和3791亿元，分别增长31.9%、19.2%、16.6%、13.9%、24.4%和22.8%，六省市

合计软件业务收入38400亿元，占全国比重为74.6%，占比较去年同期提高2.1个百分点。

中心城市软件业务收入较快增长，利润总额增长持续放缓。1—7月，全国15个副省级中心城市实现软件业务收入27299亿元，同比增长17.9%，比上年回落1.5个百分

点，占全国软件业务收入比重为53.1%，占比较去年同期回落1.7个百分点。其中，广州和济南软件业务收入同比增速超过全行业平均水平。中心城市软件业利润总额3286亿元，同比增长3.2%，比上年回落4.5个百分点。其中，西安、广州和长春的利润总额增速超过20%。



数据来源：工信部运行监测协调局

# 网络安全行业点亮“航标灯”

（上接第1版）二是健全责任范围，形成对关键信息基础设施保护工作的全方位责任保障；三是明确责任方式，主要涵盖行政责任、民事责任和刑事责任三大类别。

## 《条例》旨在解决哪些问题？

随着我国国民经济和社会信息化的全面推进，传统的社会活动不断向网络空间延伸扩展，经济与国家安全高度依赖于关键信息基础设施。“完善关键信息基础设施保护法律体系，全面提升关键信息基础设施安全保护意识、保障能力和水平，已经成为网络安全博弈的制胜关键。”陈颖明表示。

然而现阶段，我国关键信息基础设施的安全防护仍存在不少问题。华云数据控股集团高级副总裁郭晓在接受《中国电子报》记者采访时坦言：“我国整体安全投入与全球市场还存在差距。”国家统计局和IDC数据显示，我国网络安全产业占GDP仅0.41%，和美国相差3.6倍，网络安全产业规模和美国相差5.5倍。

不过，业界人士普遍认为，《条例》的出台将给国内网络安全产业带来较大增量空间。中信证券称，《条例》正式施行后有望带动省级、国家级关键信息基础设施

安全投入增加。假设国家级、省级关键信息基础设施有望达到2万个，平均每个关键信息基础设施每年的安全投入为100万元，则《条例》带来的增量市场每年预计有200亿元。

陈颖明指出：“结合近期的政策，政企安全投入比重的提升将推动网安行业开启高速增长期，预计未来安全投入与全球市场的差距将持续缩小。尤其是公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等这些《条例》要求保护的重点行业，未来将是网络安全能力建设和投入的重点。”

“除了安全投入不足，我国关键信息基础设施安全保护还面临自主可控能力不足、缺乏完善有效的脆弱性评估机制和安全恢复计划、安全风险监测和预警机制较弱等挑战。”刘权谈道。

今年5月国家互联网应急中心（CNCERT）发布的《2020年我国互联网网络安全态势综述》数据显示，勒索病毒、APT攻击、系统漏洞、数据安全等安全问题已逐渐成为企业、政府机构、金融机构等对网络安全性要求较高用户群体最为关心的核心问题之一。而关键信息基础设施网络安全事故多发，也从侧面凸显出产业生态的不完善。

《条例》的正式施行有望补足网络安全产业链的薄弱环节。刘权分析称，《条例》明确规定关键信息基础设施运营者应当落实网络安全责任，开展安全监测和风险评估，规范网络产品和服务采购活动。从这些要求看，网络安全行业中提供风险评估、等保测评以及合规性咨询等第三方服务企业将明显受益。“尤其是是近年来兴起的网络安全托管服务，会获得更大的市场增长空间。”陈颖明强调。

“《条例》对信创产业和网安行业也表达了明确支持，指出应当优先采购安全可信的网络产品和服务。因此，跨越多行业，多领域的云服务提供商作为主要对象，其中具有信创和自主知识产权特色的企业，和具有跨界整合优质网络安全方案能力的企业会更加受益。”郭晓表示。

另外，网络安全人才问题也将获得更多的关注。陈颖明认为，关键信息基础设施运营单位普遍存在网络安全人员编制少、人才流失严重、现有人员经验不足等诸多问题，《条例》的实施会带来更大的人才需求压力。“一方面，在现有人才无法满足要求的情况下，关键信息基础设施运营单位亟须引入外部网络安全人才和服务，补齐和加强网络安全力量；另一方面，也要加强内部网络安全培训。”

## 究竟应该怎么做？

传统的安全建设往往注重先进和高效的技术防御平台建设，却忽视了平台的持续运营能力和对事件的应急处置能力。大多数单位真正缺乏的是“用好安全产品”和“应对突发事件”的能力，这无论是对关键信息基础设施运营单位的安全团队还是对提供产品和服务的安全企业，都是一个需要投入精力去解决的问题。在陈颖明看来，关键信息基础设施安全保护体系的构建，将更加强调安全运营、应急处置等“软”实力的构建，要求业内企业和单位更加注重安全能力的持续、有效运作。

一方面，关键基础设施运营者在其中扮演着不可替代的重要角色。刘权建议：“运营者需重点做好以下三个方面工作。一是落实主体责任，通过建立安全保护制度、设立专门管理机构、加强网络安全意识教育等多种形式，切实保障相关资金落实，建立网络安全保障体系；二是高度重视安全保护工作，合规做好系统建设相关工作；三是定期开展网络安全检测和风险评估，发生重大安全事件应及时向相关部门报告。”

另一方面，企业与安全从业者也是重要参与者，需提供更符合实际场景需求的安全

解决方案。陈颖明谈到：“关键信息基础设施的保护体系不应再是类似等保的‘基线’式防护，而必须是有重点、有目标的针对性管控体系。安全行业从业者必须深入到不同关键信息基础设施行业的业务场景中，基于不同的行业风险考虑系统的应对措施。”

郭晓指出，从网络安全角度出发，包括内外网安全、虚拟化安全、云原生安全都是关键信息基础设施安全保护的范围；业务数据多副本机制、本地保护策略、异地备份和恢复机制都应成为企业上云的必备前提。同时，服务商也应积极对照《条例》及《网络安全法》等法律法规，担起安全合规义务和责任，主动拥抱网络安全监管，规避合规风险，并依托创新技术，不断完善网络安全防御体系，为政府和企业用户构筑起一道云上的安全屏障。

总体来看，关键信息基础设施安全保护体系的构建更强调总体规划、技术可信、持续运营和有效性监管，要求整个行业的从业者共同协作，建立更完善的产业生态体系。陈颖明认为：“这包括但不限于——规划层面，完善基于行业属性的安全标准与最佳实践；建设层面，促进安全可信技术的发展，安全产品和运营能力的规范化评价体系；运营层面，建立更顺畅的信息共享和技术协同机制，充分发挥运营者内部自查、行业监管和国家监管的多层保障和促进作用。”