北京通信信息协会会刊

共抗新冠肺炎疫情，会员在行动特刊

2020 年第 10 期 总第 699 期
北京通信信息协会秘书处编辑 2020 年 3 月 3 日

中金启动预案保复工

中金北京、烟台、昆山、武汉四地数据中心面对疫情第一时间启动“突发传染性疾病应急预案”，分别成立 “疫情防控领导小组”，工作小组下设包括办公室、员工关怀组、客户宣传组、政府联络组、工程管理组、运维保障组及后勤保障组等职能小组。各数据中心统一迅速部署，实施对新型冠状病毒感染的预防性措施。公司工程、运维、营销等部门针对项目情况制定专项应急预案，严格做到保障客户生产系统安全稳定运行，保障运维人员与客户身体健康安全。

中金各数据中心严格做好员工新冠肺炎防控记录，严格执行各项应急措施，主要包括：（1）严格限制数据中心来访，进入园区人员必须佩带口罩；（2）启动数据中心运行管理中心领导值班制度，负责 24 小时督导协调防疫工作；（3）启动“零报告制度”，统计公司全员及客户驻场人员的每日身体健康状况并向领导小组通报；（4）加强巡检与供应服务力度，确保对数据中心的服务稳定运行；（5）增加园区内公共场所消毒次数；（6）主动加强与客户的单线沟通，减少中心员工与客户接触；（7）采购并储备足够食品与生活必需品，满足常驻人员基本生活和使用需要；（8）与开发区政府、医疗机构、派出所建立密切沟通，紧急情况下联系各单位紧急处置；（9）及时向客户通报疫情情况，并说明对生产运行的可能影响。截止目前，中金四地人员无一人感染。

“通信大数据行程卡”上线服务

2 月 29 日，中国信息通信研究院联合三家基础电信企业利用电信大数据，推出“通信大数据行程卡”服务，为全国 16 亿手机用户免费提供其本人 14 天内到访地服务。

通行卡无需安装，使用便捷：手机用户可通过扫码、网页或发送短信等方式，获取本人 14 天内停留 4 小时以上的地市，根据停留情况，生成绿色或红色的通行卡。该方式基于用户授权并且经过本人实时验证，在充分保障用户隐私的条件下，方便快捷地提供查询服务。

中国信息通信研究院将配合相关政府部门，加强个人信息保护，在确保用户信息安全的前提下，做好“通信大数据行程卡”在复工复产、道路通行、出入国境等方面的使用。

“复工复产助小微”快应用上线运行

3 月 1 日，由新华社经济参考报社、中国信息通信研究院泰尔终端实验室联合中国建设银行、华为、小米、vivo、OPPO 四大手机厂商共同推出的“复工复产助小微”快应用上线运行。

快应用作为移动互联网新型应用形态与手机系统深度整合，免下载、免安装，一键触达，能够让使用者体验到“秒开”。在 5G 网络环境下，用快应用形式实现普惠金融服务，极大地推动了 5G 应用创新。“复工复产助小微”快应用功能包括：防疫专区、政策措施、贷款产品和智慧社区等，有效满足了小微企业在特殊时期对疫情防控和复工复产的需要，着力破解横亘在小微企业面前的种种痛点和难点。

启迪区块链保复产复工

启迪在疫情发生之后，紧急组织行业专家及技术团队加班加点开发并推出“公共场所体温检测精准筛查预警系统（TUS PHID 系统）”和“智慧防控小程序”等多款疫情防控产品，帮助园区、学校、医院、社区、地铁等重点公共场所实现“一体化”疫情联防联控，推动各地有序复工复产。

“一体化”疫情防控数字服务融合了区块链、人工智能、大数据和边缘计算等新一代创新技术，各项产品相辅相成，线上线下“同频共振”。智慧防控小程序和公共场所体温检测精准筛查预警系统（TUS PHID 系统）联动，实现对重点场所人员流动和体温变化的智慧化管理和监控，保障复工复产人员健康信息登记“不漏一人”，身份核查“不漏一人”，体温上报“不漏一人”，属地管控“不

漏一人”，为复工复产、人民群众健康安全提供强有力的信息化支撑，并通过大数据平台连通社区、医疗、疾控、交通、运营商等相关机构数据，建立可回溯、可跟踪、可分析、可预警的智能化疫情防控体系，有效提升各地疫情防控效率。

启迪区块链推出的“一体化”疫情防控数字服务已在北京、河北、浙江、江苏、湖南、广东、甘肃等地陆续“上岗”，为政府和企业的疫情防控工作提供技术保障，成为各地疫情防控的重要手段。

普天捐赠 5G 智能监测设备支援武汉“智慧方舱”

2 月 28 日下午，上海市科委支援湖北省防疫前线捐赠项目对接视频会在中科院上海微系统与信息技术研究所举行。在获悉上海市科委和湖北省科技厅的需求后，总经理陶雄强高度重视并亲自部署落实，要求迅速研究制定“5G 智慧应用”捐赠方案并启动捐赠工作。

普天技术快速，联合义金健康针对武汉市方舱医院的患者智能护理、医务人员智能防护核心需求，制定了基于物联网、5G、大数据、人工智能等技术，面向患者、医护人员的 5G 智能体征监护系统产品和解决方案，捐赠 5G 智能监护平台、医务人员健康监测平台，以及智能床垫、智能体温贴、腕式脉搏血氧仪、智能血氧指环等可穿戴、无拘束智能体征监测产品，总价值为 130 余万元，助力武昌方舱医院实现疫情全方位防控。

5G 智能体征监护系统具有以下几个功能：（1）实时体温、血氧、呼吸、心率等体征监测，在床/离床状态展示；（2）异常时主动预警，可以查看最近一周的异常提醒；（3）24 小时不间断体征监测和历史数据展示。系统一方面，能够通过物联网监测设备对患者进行远程实时体征数据采集，将体温、血氧、呼吸、心率等体征数据实时上传至云平台，医护人员可通过监控中心、护士站监控大屏等及时获知患者体征情况。另一方面，医护人员也可佩戴智能体温贴和血氧指环，通过手机 APP 实现体温和血氧数据的实时上传和连续监测，及时获知自身体征情况，从而起到保护医务人员健康安全的作用。

为抗击疫情，早在 1 月 23 日，中国普天与合作伙伴义金健康为上海市公共卫生临床中心部署了“5G 动态体温监护系统”及 200 余套体温检测设备，系统采用 5G 传输+智慧医疗数据云平台技术，有效提高了一线医护队伍的战斗力。

兆维集团推出“身份验证&体温筛查”人员管理解决方案

兆维集团研发了基于虹膜识别及人脸识别技术，应用红外热像测温技术的“身份验证&体温筛查”人员管理解决方案。虹膜识别的引入很好地解决疫情期

间因为人面部佩戴口罩对人脸识别准确率的影响。方案目前已在工业园区、政务大厅等商务办公楼宇布放，为有效控制疫情，保障复工复产，提供有力技术支持。

“京科惠农”网络大讲堂服务草莓种植

受疫情影响，当前草莓生产和销售都面临不同程度的困难。为了解决草莓产业面临的问题，2020 年 2 月 27 日上午，“京科惠农”网络大讲堂第二期网络直播在北京市农林科学院信息与经济所演播室如期开播，特别邀请我院林果院、北京市草莓工程技术研究中心草莓专家张运涛研究员，针对北京特色草莓产业的发展问题进行专业指导，解读产业困境，解决技术问题，促进产业增效。

本期主题为“面对疫情草莓产业面临的问题和对策”， 针对京郊特色草莓产业的现状和关键问题，作为资深草莓专家的张运涛研究员从产业发展角度，重点讲解了日光温室草莓管理关键技术和育苗管理技术，分享应用网上营销渠道，促进网络营销；结合部分地区草莓滞销的问题，介绍了草莓酿酒和速冻草莓等草莓加工技术，为滞销草莓指出新出路，缓解目前发展的瓶颈问题。直播中，用户提出了大量草莓生产中的技术问题，张老师结合自己丰富的研究和生产经验，进行了细致的解答，受到用户的强力点赞。

北京移动落地北京市首例 5G 无人驾驶防疫消毒车应用

疫情期间，北京移动与首都医科大学附属北京潞河医院合作，成功落地北京市首例 5G 无人驾驶防疫消毒车应用。5G 无人驾驶防疫消毒车“蜗小白”通过 5G+物联网和人工智能技术，运用清扫消毒过程无人化、无人驾驶持续作业、智能语音播报等创新功能，实现对院区近 6 万平米的全面自动化清扫和消毒，成功地解决了疫情期间医院面临的隔离难、清洁工荒、消毒难三大难题，大大降低人工清扫消毒的感染风险，提升了工作效率。特别是 5G 无人驾驶防疫消毒车搭载中国移动 4G/5G 网络，实现无人驾驶和远程驾驶，真正地达到了足不出户，消毒于千里之外的目的。

亚信科技“翼知疫行”助力运营商

亚信科技疫情期间开发的“翼知疫行”APP 为政府及个人提供了包括区域风险查询、疫情预测查询、返城报告查询、行程查询和接触查询等功能。在保证用户隐私安全的基础上，“翼知疫行”对重点疫情地区人员流动情况进行实时感知，配合相关省份重点开展对定点医院、发热门诊、人员聚集区等重点区域的人流变化分析，为有关部委、部分省市政府提供疫情防控相关人口流动大数据分析支撑

服务，协助政府提供开放透明的数据，打消公众对周边疫情的恐惧。“翼知疫行”APP 目前使用人次超过 1000 万，被中国电信作为服务公众的重点应用服务产品在相关省市中进行推广。

=行业思考=

从“删库”事故，浅谈企业如何防范及应对数据安全事件

近日，国内某大型上市微商城服务提供商发生重大“删库”事件，导致约 300 万家商户生意基本停摆，该公司平台自中断服务至完成修复历时长达 168 小时，损失惨重。

此前也不乏类似事件发生。国内某大型在线旅行服务公司由于服务器遭受不明攻击，导致网站及 APP 陷入瘫痪，相关服务器数据在此次故障中全部被物理删除且备份数据无法使用。某内容创业型公司长期沉淀用户及内容数据由于故障全部丢失，对于该公司无疑是一次毁灭性打击。

近年来，随着数字经济的快速发展，数据的价值持续升高，数据安全也面临着更大的风险和挑战。对于企业来说，无论是何种原因造成的数据安全事故，都将会为业务运转、经营收入、企业形象、用户隐私等方面带来不良影响和危害。对于以数据作为核心资产的企业来说，更应引起足够重视。

那么对于企业来说如何面对未来有可能出现的数据安全挑战？联通大数据有限公司携手联通智慧安全科技有限公司，针对双方在数据安全方面的实践经验进行分享。

一、事前预防，事中控制，事后总结

“事前预防”是关键。要尽可能地做到“未雨绸缪，防患未然”。这一阶段可主要考虑以下内容：

1、以资产维度，进行必要的“风险评估”以及“风险管理”。全面梳理企业所面临的安全风险都有哪些，以及针对这些安全风险所采取的具体措施。

2、根据“风险评估”和“风险管理”的输出结果，企业需要准备相应的预

算在“人员、流程、技术”三个方向进行投入。

3、针对“组织、团队、人员”方面，至少需要考虑以下工作内容：加强对公司全体员工的安全意识培训；加强对开发人员的代码安全规范的培训；加强对运维人员的操作规范及法律知识的培训；基于“职责分离（Separation of Duty）”以及“最小权限（Least Privilege）”等安全原则，对组织架构、团队分工、人员职责、角色划分等进行必要的梳理和调整；等等。

4、针对“技术、产品、平台”方面，至少需要考虑以下工作内容：全面梳理企业的互联网暴露面；全面梳理企业的 IT 资产，对重要的数据资产进行分级、分类管理；完善脆弱性风险管理机制，实现脆弱性的闭环管理；逐步健全企业的安全运营平台，以及安全运营平台所需要的技术、产品等，为后面的“事中控制”以及“事后总结”提供必要的技术和数据支撑；针对企业关键的数据资产，建立数据的在线备份、离线备份机制，并且定期进行针对备份数据的恢复测试；等等。

5、针对“流程、制度、标准”方面，至少需要考虑以下工作内容：完善企业的“授权管理流程”、“应急响应与应急处置流程”、“业务与数据恢复流程”等关键性流程、制度；参考国家、行业监管单位对于企业的安全要求，完善自身的安全建设；建立适合企业自身的“安全标准”，从企业 IT 发展的方方面面进行规范化管理；等等。

“事中控制”是核心。这个阶段有两个非常重要的指标,“平均检测时间(Mean Time To Detect，MTTD）”以及“平均响应/修复时间（Mean Time To Response/Repair，MTTR）”。在“事前预防”阶段做的越好、越到位，MTTD/MTTR 这两个指标就会越小（例如：分钟或者小时级别），企业的损失也会降到最少；反之,如果在“事前预防”阶段做的不好,或者根本没有任何准备,那么,MTTD/MTTR 这两个指标就会非常不理想（例如：天或者周级别），企业的损失也会非常严重。

“事后总结”是保障。每次“发现问题、解决问题”的过程都是对“事前预防”阶段所有工作的一次验证，从中必定可以发现很多不完善的地方，例如:员工安全意识不够、缺乏技术手段、某个流程中缺少重要环节等，这也就是需要持续改进的内容。只有“善于总结、持续迭代”，企业才能维持一个相对健康的安全体系，所以说这个阶段是企业安全的保障。

二、类似事件，我们会如何做？

在服务过程中，我们也曾不可避免地发生过类似的数据丢失事件：在某次日常安全巡检过程中，审计系统发出异常警报，安全巡检人员初步判定为数据安全事件后，立即报告安全负责人，迅速组成应急处置小组，启动应急预案，在保存当前环境后，运维人员对异常节点执行数据恢复，同时安全技术人员通过监控记录、日志审计定位异常原因为某员工过失执行删除命令，最后根据公司问责制度对该员工进行了通报处置。

此次数据损坏事件从发现到数据恢复正常不超过 1 个小时，整个事件的处置过程不超过 4 个小时，事件发生时，系统及时自动启动了备份数据，并未对公司业务造成影响。我们之所以能够沉着应对数据安全事件、并做到高效处置的原因，就是基于公司在数据安全防护能力及集群自动化运维能力方面的沉淀。

联通大数据公司构建了“零信任”的数据全生命周期的大数据安全防护体系，体系基于安全组织、安全制度、安全技术和安全运营四个维度，可有效减少数据安全事件发生的可能性，一旦事件发生后，可大大降低因事件发生所造成的损失。

我们将视角拉回本文开头发生的数据破坏事件，应用联通大数据全生命周期的大数据安全防护体系，将如何防护避免此类意外发生？

1、在安全组织层面，建立完善的数据安全责任体系，将安全巡检、数据备份、安全培训等重要的数据安全防护环节落实到岗位人员，明确职责划分。

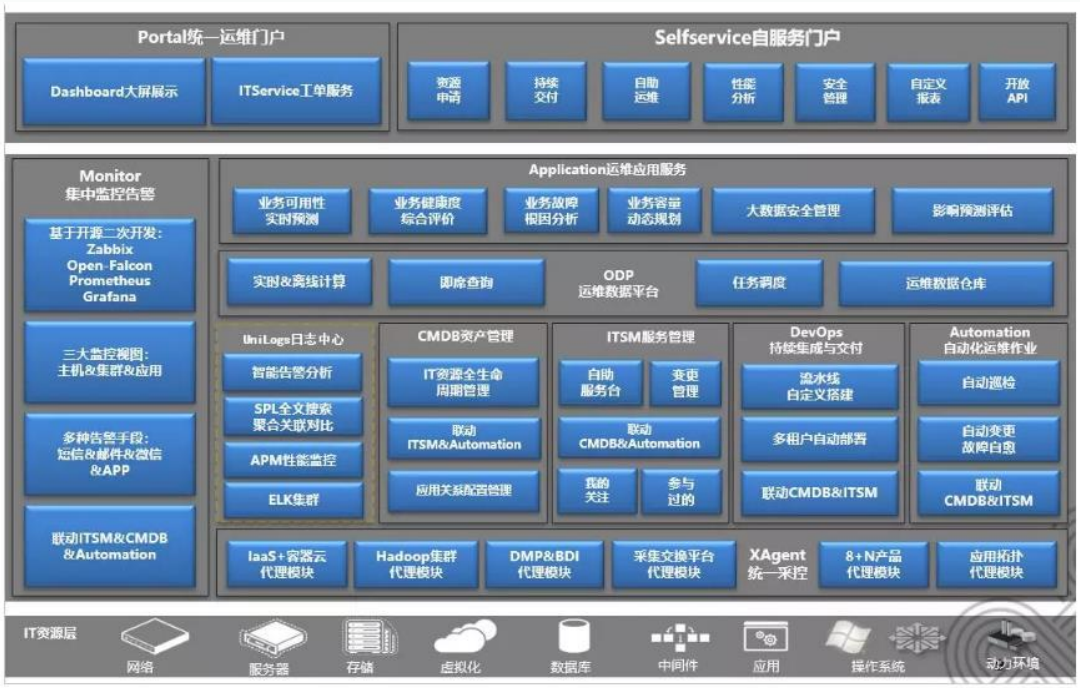
2、在安全制度层面，第一，制定数据丢失损坏事件的应急处置预案，定期进行应急演练，不断验证数据备份和恢复机制的有效性，保证应急预案的可操作性；第二，建立有罚有赏的问责机制，充分发挥问责的“震慑”作用；第三，建立定期安全培训机制，尤其加强对重要岗位人员的安全意识、法律意识和安全能力的培训。

3、在安全技术层面，第一，通过统一账号认证授权审计系统严格控制人员对数据的访问和操作权限，保证“最小授权”，并严格限制特殊权限授权，例如：“root”、“admin”等；第二，通过安全审计系统对人员的操作行为，例如：“rm -rf”和“fdisk”等高危操作，进行实时监控和报警，限制高危操作行为。

4、在安全运营层面，严格按照公司制度流程要求，充分利用安全技术能力，实施精细化数据安全运营，保证事前、事中、事后全闭环管控，严格把控数据安全的风险。

三、更安全的自动化运维思路

安全是运维工作中不可或缺的责任，针对人工带来的不确定因素风险，联通大数据公司建立了一套端到端的自动化运维体系，保障重要业务数据的自动备份和恢复机制，增强系统容错能力。



典型的自动化运维体系架构

构建自动化运维体系的核心要点有以下三点：

1、实现全平台多集群应用统一监管：解决分散集群应用运维难题，采用统一的 PaaS 应用入口，做到权限集中管理，采用多维度监控方式，例如：主机监控，组件监控，服务拨测，日志监控，脚本监控。对于微服务，采用应用链路调用拓扑监控方式，便于故障排查。此外多种业务日志可采用图形化方式进行展示。

2、实现应用消费为中心的 IT 资源管理平台：以应用为中心的资源管理模型，建立 IT 资源管理驱动力。服务集中管理在容器中，自动化编排，减少部署和运维成本，降低人为操作带来的失误。将传统的低级自动发现结合现有的故障自愈系统，尽可能做到了 IT 资源自动化。

3、实现应用持续交付的自定义流水线：基于持续集成与交付模式开发测试和上线应用 SmartOps，配合作业种类统一管理的作业平台，拥有细粒度的主机与用户组权限，对 Gitlab 仓库权限精细控制，有灵活多样的任务原子调度，完善的代码检测机制，多种脚本执行方式，大大降低运维人力投入，可进行人工审核，配置自动化定期备份，拥有详尽的历史记录和完整的审计日志等，在安全方面做到巨细无遗。

文中提到的删库事件，看似是简单的数据库被删、数据丢失，但实际反映出的却是目前多数企业对数据安全缺乏了解，如何有章法地、循序渐进地、在预算范围内保障安全，是整个行业都需重视和思考的问题。

（联通大数据供稿）


BITA