炼石
CipherGateway

2021 数据安全与个人信息保护技术白皮书

北京炼石网络技术有限公司

2021.11.1

声　明

北京炼石网络技术有限公司对本技术报告内容及相关产品信息拥有受法律保护的著作权，未经授权许可，任何人不得将报告的全部或部分内容以转让、出售等方式用于商业目的使用。转载、摘编使用本报告文字或者观点的应注明来源。报告中所载的材料和信息，包括但不限于文本、图片、数据、观点、建议等各种形式，不能替代律师出具的法律意见。违反上述声明者，本公司将追究其相关法律责任。报告撰写过程中，为便于技术说明和涵义解释，引用了一系列的参考文献，内容如有侵权，请联系本公司修改或删除。

北京炼石网络技术有限公司

联系电话：4008190181

邮箱：support@ciphergateway.com

前　言

当前，以数字经济为代表的新经济成为经济增长新引擎，数据作为核心生产要素成为了基础战略资源，数据安全的基础保障作用也日益凸显。伴随而来的数据安全风险与日俱增，数据泄露、数据滥用等安全事件频发，为个人隐私、企业商业秘密、国家重要数据等带来了严重的安全隐患。近年来，国家对数据安全与个人信息保护进行了前瞻性战略部署，开展了系统性的顶层设计。《中华人民共和国数据安全法》于 2021 年 9 月 1 日正式施行，《中华人民共和国个人信息保护法》于 2021 年 11 月 1 日正式施行。

本白皮书（或本报告）正是在《数据安全法》、《个人信息保护法》等法律陆续施行的背景下编制。《数据安全法》旨在维护国家安全和社会公共利益，保障数据安全，其关于“数据”的定义，是指任何以电子或者其他方式对信息的记录。《个人信息保护法》更侧重于个人权益，是为了维护公民个人的隐私、人格、人身、财产等利益，其关于“个人信息”的定义，是指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

业内关于“数据”和“信息”之间关系的理解，大致可以分为三类：一是“信息”属于“数据”的子概念，“信息”是从采集的“数据”中提取的有用内容；二是“信息”与“数据”互相混用，概念区分没有实质意义；三是“数据”属于“信息”的子概念，仅表示“信息”在电子通信环境下的表现形式。本报告基于数据和信息之间关系的第一种释义，即“个人信息”属于“数据”的子概念。同时，《数据安全法》中的数据处理者在处理个人信息时，也是《个人信息保护法》

中的个人信息处理者，除需遵守《数据安全法》，还必须遵守《个人信息保护法》。从技术层面看，个人信息往往以结构化数据或非结构化数据形式存在，保护个人信息和保护数据的防护手段，二者高度通用。综合考虑以上原因，本报告将数据安全技术与个人信息保护技术合并论述。

本报告综合梳理了当下数据安全发展面临的挑战与机遇，结合真实的数据泄漏事件，分析业务流转各环节伴生的安全风险与应对，探索数据安全“新框架”与“新战法”。本报告参考经典的网络安全框架 ATT&CK，提出了新的数据安全技术框架 DTTACK（以数据为中心的战术、技术和通用知识），以期结合两大框架实现“攻防兼备、网数一体”。本报告详细介绍了 DTTACK 框架，针对数据安全从识别（I）、防护（P）、检测（D）、响应（R）、恢复（R）、反制（C）、治理（G）七大方面说明了相应的战术、技术，覆盖了数据的全生命周期（收集、存储、使用、加工、传输、提供、公开等）的安全防护。最后，报告从云平台、工业互联网、政务大数据、银行金融、民航业等十个场景，简要阐述了数据安全的应用示例方案以供参考。

“工欲善其事，必先利其器”，在数字经济快速发展的背景下，我们更需要深刻认识到数据安全建设的重要性，不仅需要在安全意识和管理水平上提升，更需要在技术上重点布局、勇于创新，希望本报告能够为企业或机构的数据安全建设提供参考和借鉴。由于编者水平有限，报告中的错误之处在所难免，敬请读者指正，也欢迎业界同仁共同参与完善，为行业发展提供助力！

目录

图目录

表目录

一、数据安全发展面临严峻挑战

1.1 数据要素赋能数字中国

1.1.1 数据成为新型生产要素

2020 年 4 月 9 日，中共中央、国务院印发《关于构建更加完善的要素市场化配置体制机制的意见》（以下简称《意见》），提出土地、劳动力、资本、技术、数据五个要素领域的改革方向和具体举措。数据作为一种新型生产要素写入中央文件中，体现了互联网大数据时代的新特征。当前数字经济正在引领新经济发展，数字经济覆盖面广且渗透力强，与各行业融合发展，并在社会治理中如城市交通、老年服务、城市安全等方面发挥重要作用。而数据作为基础性资源和战略性资源，是数字经济高速发展的基石，也将成为“新基建”最重要的生产资料。数据要素的高效配置，是推动数字经济发展的关键一环。加快培育数据要素市场，推进政府数据开放共享、提升社会数据资源价值、加强数据资源整合和安全保护，使大数据成为推动经济高质量发展的新动能，对全面释放数字红利、构建以数据为关键要素的数字经济具有战略意义。

在数据时代，以大数据为代表的信息资源向生产要素形态演进，数据已同其他要素一起融入经济价值创造过程。与其他资源要素相比，数据资源要素具有如下特征：一是数据体量巨大。且历史数据量不断累积增加，通过流转和共享对社会发展产生重要价值，基于数据创新的商业模式或应用不断演进。二是数据类型复杂。不仅包含各种复杂的结构化数据，而且图片、指纹、声纹等非结构化数据日益增多；三是数据处理快，时效性要求高。通过算法对数据的逻辑处理速度非

常快，区别于传统数据挖掘，大数据处理技术遵循“一秒定律”，可以从各种类型的数据中快速获得高价值的信息。四是数据价值密度低。数据价值的高度与精确性、信噪比有关，在海量数据面前有价值的数据所占比例很小。在获取高价值数据的过程中，往往需要借助数据挖掘等方法深度分析海量数据，从中提取出对未来趋势与模式预测分析有价值的数据。

基于以上四个特性分析，数据在参与经济建设、社会治理、生活服务时，具有重要意义。一是数据作为一种生产性投入方式，可以大大提高生产效率，是新时期我国经济增长的重要源泉之一。二是推动数据发展和应用，可以鼓励产业创新发展，推动数据与科研创新的有机结合，推进基础研究和核心技术攻关，形成数据产业体系，完善数据产业链，使得大数据更好服务国家发展战略。三是数据安全是数据应用的基础。保护个人隐私、企业商业秘密、国家秘密等。在加强安全管理的同时，又鼓励合规应用，促进创新和数字经济发展，实现公共利益最大化。从合规要求看，数据安全成为国家顶层设计，相关法律政策明确提出加强网络安全、数据安全和个人信息保护，数据安全产业迎来前所未有的历史发展机遇。最终用户对于主动化、自动化、智能化、服务化、实战化的安全需求进一步提升，在此需求推动下，数据安全市场未来五年将继续维持高增速发展。根据赛迪咨询数据测算，2021 年我国数据安全市场规模为 69.7 亿元，预测在 2023 年我国数据安全市场规模将达到 127 亿元。从实战需求看，日趋严峻的网络安全威胁让企业面临业务风险，数字产业化迫切需要数据安全能力，而产业数字化转型带来数据安全新需求。当前，我国数据安全产业处于起步期，相比于西方发达国家，我国尚有很大增长潜力，这既是短板也是市场机会。随着实战化和新合规的要求逐步深入，数据安全将迎来广阔的市场空间。

1.1.2 数据开发利用加速发展

当前，数据要素成为推动经济转型发展的新动力。通过数据流引领技术流、物资流、资金流、人才流，推动社会生产要素的网络化共享、集约化整合、协作化开发和高效化利用，提升经济运行水平和效率。特别是后疫情时代，数字产业化和产业数字化将推动数据开发利用的需求从被动变为主动，从启动变为加速，迎来蓬勃发展的黄金时代。

政府数据开放共享，推动资源整合，提升治理能力。随着国家顶层设计和统筹规划，政府依托数据统一共享交换平台和政府数据统一开放平台，大力推进中央部门与地方政府条块结合、联合试点，实现公共服务的多方数据安全共享、制度对接和协同配合；通过政务数据公开共享，引导企业、行业协会、科研机构、社会组织等主动采集并开放数据，提升社会数据资源价值、加强数据资源整合和安全保护。同时，优化数据开发利用，不断提升大数据基础设施建设、宏观调控科学化、政府治理精准化、商事服务便捷化、安全保障高效化、民生服务普惠化。

推动产业创新发展，培育新兴业态，助力经济转型。随着 5G、云计算、大数据、人工智能等新技术的发展，以及互联网金融、数据服务、数据探矿、数据化学、数据材料、数据制药等新业态的加速兴起，提升了数据资源的采集获取和分析利用能力，充分发掘数据资源支撑创新的潜力。同时，工业大数据、农业农村大数据、万众创新大数据、基础研究和核心技术攻关等同步蓬勃发展，围绕数据采集、整理、分析、发掘、展现、应用等环节，打造较为健全的大数据产品体系，带动技术研发体系创新、管理方式变革、商业模式创新和产业价值链体系重构，推动跨领域、跨行业的数据融合和协同创新。

强化安全保障，提高管理水平，促进健康发展。数据开发利用升级离不开数据安全的保障。加强数据安全问题研究和安全技术研究，落实商用密码应用安全性评估、信息安全等级保护、网络安全审查等网络安全制度，建立健全大数据安全保障体系。建立大数据安全评估体系。同时，采用安全可信产品和服务，提升基础设施关键设备安全可靠水平，强化安全支撑。[2]

1.2 个人信息亟待严格保护

1.2.1 个保法律强化保护义务

个人信息作为数据资源的重要组成部分，应该受到严格保护。但过去由于传统观念、信息环境、技术手段和立法规划等方面的原因，我国的个人信息保护一直没有得到应有的重视，也没有制定专门针对个人信息保护方面的法律。

2021 年 11 月 1 日，《中华人民共和国个人信息保护法》正式实施。《个人信息保护法》就“个人信息处理规则”、“个人信息跨境提供的规则”、“个人在个人信息处理活动中的权利”、“个人信息处理者的义务”、“履行个人信息保护职责的部门”等，以及相关各方的“法律责任”作出了明确界定。该法统筹私人主体和公权力机关的义务与责任，兼顾个人信息保护与利用，为个人信息保护工作提供了清晰的法律依据。《个人信息保护法》是我国保护个人信息的基础性法律，奠定了我国网络社会和数字经济的法律之基。

个人信息受到应有的保护是社会文明进步的重要标志之一，也是我国法制建设与国际接轨的有力举措。《个人信息保护法》借鉴国际立法经验，结合本国经济社会实际，是中国智慧的结晶。该法必将在保护个人权益，促进经济社会稳定发展方面发挥重要作用。

1.2.2 个人信息需要体系防护

目前，我国个人信息的安全状况相当严峻。基于个人信息所蕴含的巨大商业价值，加上数字经济带来了新变化，个人信息安全事件呈现出大幅上升的势头。掌握大量个人信息的商业银行、电信运营商、电商平台、交通旅游业企业等成为案发重灾区，相关案例屡屡见诸媒体。这就要求与个人信息相关的行业企业，提高对个人信息保护工作重视程度，依照个人信息保护法要求，建立起行之有效的保护体系。基本措施包括：

1）建立和完善相关的组织机构

《个人信息保护法》具有强制力，相关部门和单位应该依照法条要求，制定和落实保护计划。只有建立高效的组织，制定科学的制度，积极采取行动，使措施落地，个人信息的安全才能依法得到保证。

2）加强个人信息保护技术的应用

数字经济能够产生高附加值的重要原因之一是数据资源的共享。大数据、云计算、区块链等新技术的应用，使得网络“边界”难于划分，原有的基于传统信息安全保护思路，注重固定“边界”攻防的技术手段，已难于满足当前个人信息保护的需求。新老问题叠加，需要新的信息安全保护思路和技术手段，积极采用加密与去标识化等技术，才能有效应对新的安全威胁，这对个人信息保护工作提出了新挑战。

3）落实个人信息处理者责任

对于个人信息安全事件的追责不力是导致个人信息安全事件频发的重要原因之一。伴随个人信息保护法的出台，众多涉及个人信息的处理者都将共同参与

行动，与之配套的就是要落实责任。结合各单位的具体情况，应该设立个人信息保护责任人，设立奖惩制度。只有责任到人，才能踏石留印，抓铁有痕，见到实效。

1.3 业务处理伴生数据风险

数据这种新型生产要素，是实现业务价值的主要载体，数据只有在流动中才能体现价值，而流动的数据必然伴随风险，数据安全威胁伴随业务生产无处不在。因此，凡是有数据流转的业务场景，都会有数据安全的需求产生。传统认为，安全和业务是关联的，有时候对立。但换个角度，安全其实就是一种业务需求。“传统业务需求”侧重于“希望发生什么”，而“安全需求”则侧重于“不希望发生什么”，从而确保“发生什么”。从业务视角出发，数据安全需求重点是数据的机密性和完整性。

结合到企业或机构的信息系统中，数据安全则来自于业务处理中的风险映射。从时间维度看，数据在流转的全生命周期中的每个环节都会有相应的安全需求；从空间维度看，数据在基础设施层、平台层以及应用层之间流转，不同层次会有不同颗粒度的防护需求。《数据安全法》提出“数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等”，为数据生命周期的各环节提供了明确定义，数据在各环节均面临诸多泄露威胁与安全挑战。

1.3.1 数据收集风险

在数据收集环节，风险威胁涵盖保密性威胁、完整性威胁、可用性威胁等。保密性威胁指攻击者通过建立隐蔽隧道，对信息流向、流量、通信频度和长度等

参数的分析，窃取敏感的、有价值的信息；完整性威胁指数据与元数据的错位、源数据存有恶意代码；可用性威胁指数据伪造、刻意制造或篡改。

(1)国内

1）某程集团因涉嫌违规采集个人信息被诉至法院

司法机关：浙江省绍兴市柯桥区人民法院

案例描述：2021 年 7 月，浙江省绍兴市柯桥区人民法院开庭审理了胡某诉上海某程集团侵权纠纷案件。胡某以上海某程集团采集其个人非必要信息，进行“大数据杀熟”等为由诉至法院，要求某程集团 APP 为其增加不同意“服务协议”和“隐私政策”时仍可继续使用的选项。法院审理后认为，某程集团的“服务协议”和“隐私政策”以拒绝提供服务形成对用户的强制。其中，“服务协议”和“隐私政策”要求用户特别授权某程集团及其关联公司、业务合作伙伴共享用户的注册信息、交易、支付数据并允许某程集团及其关联公司、业务合作伙伴对其信息进行数据分析等内容属于非必要信息的采集和使用，无限加重了用户个人信息使用风险。据此，法院判决某程集团应为原告增加不同意其现有“服务协议”和“隐私政策”仍可继续使用的选项，或者为原告修订“服务协议”和“隐私政策”，去除对用户非必要信息采集和使用的相关内容，修订版本须经法院审定同意。[3]

2）速贷之家主体智借网络贩卖个人信息被罚

执法机构：江苏省仪征市人民法院

法律依据：《中华人民共和国刑法》第二百五十三条之一第一、四款，第二十五条第一款，第二十六条第一、四款，第二十七条，第六十七条第一、三款，第四十五条，第七十二条第一、三款，第七十三条第二、三款，第五十二条，第五十三条第一款，第六十四条和《中华人民共和国刑事诉讼法》第十五条

案例描述：2016 年，贤某成立北京智借网络科技有限公司（简称“智借网络”），并担任法定代表人，从事贷款超市等业务。2018 年 1 月至 2019 年 7 月间，贤某与公司技术部负责人赵某等人共同商议孵化“一键贷”项目。在明知公司没有贷款资质的情况下，贤某及相关负责人仍开发“一键贷”贷款申请页面投放网络，诱骗他人申请注册，收集个人信息，在未取得受害人同意的情况下，向下游多家不特定信息服务公司出售包含姓名、身份证号、手机号等个人信息，非法盈利共计 316.96 余万元。买方涉及多家知名公司，如平安普惠、拍拍贷、你我贷等。最终法院判决智借网络犯侵犯公民个人信息罪，判处罚金 320 万元。主犯贤某犯侵犯公民个人信息罪，判处有期徒刑三年，缓刑三年，并处罚金 30 万元。[4][5]

(2) 国外

1）ZOOM 因涉嫌非法泄漏个人数据而被起诉

法律依据：《加州消费者隐私法》

案例描述：根据 2020 年 4 月在加利福尼亚州圣何塞市联邦法院提起的诉讼，用户安装或打开 Zoom 应用程序时收集信息，并在没有适当通知的情况下将其共享给包括 Facebook 在内的第三方。Zoom 的隐私权政策并未向用户说明其应用程序包含向 Facebook 和潜在的其他第三方披露信息的代码。投诉称，该公司的“程序设计和安全措施完全不足，并将继续导致未经授权而泄露其用户个人信息”。

根据《加州消费者隐私法》规定，任何消费者如其在第1798.81.5节（d）条（1）款（A）项下所定义的未加密和未经处理的个人信息，由于企业违反义务而未实施和维护合理安全程序以及采取与信息性质相符的做法来保护个人信息，从而遭受了未经授权的访问和泄露、盗窃或披露，则消费者可提起民事诉讼并请求。为每个消费者每次事件赔偿不少于一百美元(100美元)且不超过七百五十美元(750美元）的损害赔偿金或实际损害赔偿金，以数额较大者为准。

1.3.2 数据存储风险

在数据存储环节，风险威胁来自外部因素、内部因素、数据库系统安全等。外部因素包括黑客脱库、数据库后门、挖矿木马、数据库勒索、恶意篡改等，内部因素包括内部人员窃取、不同利益方对数据的超权限使用、弱口令配置、离线暴力破解、错误配置等；数据库系统安全包括数据库软件漏洞和应用程序逻辑漏洞，如：SQL注入、提权、缓冲区溢出；存储设备丢失等其他情况。

(1)国内

1）某东电商平台确认12G用户数据泄漏

案例描述：2016年2月，国内媒体一本财经报道称一个超过12G的数据包正在黑市流通，数据包信息包括用户名、密码、真实姓名、身份证号、电话号码、QQ号、邮箱等多类个人用户信息。这个数据包已在黑市上明码交易，价格在10万-70万不等，黑市买卖双方表示该数据包来源为某电商平台。某东电商平台表示，黑客利用了Struts 2的漏洞对某电商平台数据库进行了拖库。[6]

2）济南20万孩童信息以每条一两毛被打包出售

案例描述：2016 年，济南 20 万名孩童信息被打包出售，每条信息价格一两毛。泄漏信息包括孩子的姓名、年龄、性别、父亲姓名以及父母联系电话、家庭住址（全部精确到户）等。济南警方侦破案件，系黑客入侵免疫规划系统网络，4 名嫌犯被抓获。[7]

3）机锋论坛 2300 万用户信息泄露

执法机构：北京市第一中级人民法院

法律依据：《个人信息保护法》第五十一条、第六十六条

案例描述：2015 年 1 月，互联网安全漏洞平台漏洞盒子发布消息称，国内最大的安卓论坛机锋论坛 2300 万用户数据遭泄露，包含用户名、密码、邮箱。据《个人信息保护法》规定，个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失。有相关违法行为，情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照。机锋论坛掌握众多用户个人信息和敏感个人信息，应采取相关技术保护个人信息安全，防止用户信息泄漏。[8]

4）乌云漏洞报告某易用户数据库疑似泄露（亿级）

执法机构：北京市第一中级人民法院

法律依据：《网络安全法》第 42 条

案例描述：2015 年 10 月，国内安全网络反馈平台 WooYun(乌云)发布消息称，某易的用户数据库疑似泄露，影响数量共计数亿条，泄露信息包括用户名、MD5 密码、密码提示问题/答案(hash)、注册 IP、生日等。某易邮箱过亿数据泄漏(涉及邮箱账号/密码/用户密保等)。根据《网络安全法》第 42 条相关规定，网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。某易产品收集大量用户信息和重要数据，应该采取相关措施保护数据安全，防止数据泄露事件发生。[9]

5）非法获取公民的电话信息 10 万多条

案号：（2020）冀 0681 刑初 507 号、（2021）冀 06 刑终 180 号

法律依据：《中华人民共和国刑法》第二百五十三条之一、第六十七条第三款、第六十四条、第七十二条第一款，《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》第三条第二款、第五条，《中华人民共和国刑事诉讼法》第二百零一条，《最高人民法院关于适用<中华人民共和国刑事诉讼法>的解释》第三百六十五条，《中华人民共和国网络安全法》第七十六条第五项，《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》第一条

司法机关：河北省保定市中级人民法院

案例描述：2020 年 5 月份至 8 月份，被告人刘某花 8000 元在网上购买“北斗创客”软件，通过该软件非法获取公民的电话信息 10 万多条。2020 年 7 月份，刘某通过 QQ 联系被告人高某欲购买公民个人信息数据，后被告人高某分两次以 1000 元的价格出售给被告人刘某公民个人信息数据 6 万多条。判决如下：判决如下：被告人刘某犯侵犯公民个人信息罪，判处有期徒刑三年，并处罚金人民币五千元；被告人高某犯侵犯公民个人信息罪，判处有期徒刑三年，缓刑五年，并处罚金人民币五千元。[10]

(2)国外

1）Facebook 证实 4.19 亿用户的电话信息被泄露

案例描述：2019 年 9 月 Facebook 证实，存储了超 4 亿条与 Facebook 账户关联的电话号码数据库被曝光，每条记录都包含一个用户的 Facebook ID 和连接到他们账户的电话号码。同样，2018 年 3 月“剑桥分析丑闻”首次被曝光——Facebook8700 万用户数据泄露，一家名为剑桥分析的公司通过这些数据影响了美国选举。最终，美国联邦贸易委员会（FTC）宣布与 Facebook 就该事件达成一项 50 亿美元的和解协议。

2）微软泄露 2.5 亿条客户支持记录和 PII（个人验证信息）

案例描述：2020 年 1 月，微软意外地在网上曝光了 2.5 亿条客户服务和支持记录。泄漏的数据包含客户电子邮件地，IP 地址，地点，CSS 声明和案例的描述，案例编号，解决方案和备注等。微软确认此数据泄漏，并揭示此问题是由微软内部案例分析数据库的配置错误而导致。

3）5700 万名优步司机信息遭泄露

执法机构：美国伊利诺伊州司法部

法律依据：《国家消费者保护法》

案例描述：据环球网科技综合 2018 年 9 月报道，美国科技公司优步 2016 年泄漏约 5700 万名乘客与司机个人资料，在长达一年的时间里，优步未能通知司机该平台遭受黑客袭击导致司机们个人信息被泄漏一事，而且隐瞒盗窃证据，并向黑客支付赎金以确保数据不会被滥用。美国 50 州及华盛顿特区官员向该公司提起集体诉讼，之后优步与各州达成和解协议。2018 年 9 月优步宣布：将支付 1.48 亿美元罚金，并承诺加强数据安全管理。和解要求优步遵守维护个人信息的国家消费者保护法，并在发生信息泄漏情况下立即通知相关部门，保护第三方平台用户数据，并制定强有力的密码保护政策。优步还将聘请一家外部公司对优步的数据安全进行评估，并按照其建议进一步加固数据安全。

4）美国第二大医疗保险公司 Athem 泄露 8000 万个人信息

法律依据：《国家消费者保护法》

案例描述：人民网旧金山 2015 年 2 月 5 日报道，美国第二大医疗保险公司 Anthem（安塞姆）2 月 5 日向客户发邮件称，公司数据库遭黑客入侵，包括姓名、出生日期、社会安全号、家庭地址以及受雇公司信息等 8000 名用户个人信息受到影响。这已经不是 Anthem 第一次遭遇黑客攻击。另据 Threatpost 网站 2017 年 8 月 1 日报道，2017 年 7 月，Anthem 就此次信息泄露事件达成了 1.15 亿美元的和解。

5）雅虎曝史上最大规模信息泄露 5 亿用户资料被窃

案例描述：2016 年 9 月，美国互联网公司雅虎证实，至少 5 亿用户的账户信息在 2014 年遭黑客盗取，创造了史上最大单一网站信息遭窃的纪录，泄漏信息包括：受影响用户的姓名、邮箱地址、电话号码、出生日期、密码以及部分取回密码时的安全问题。受事件影响，雅虎股票午盘下跌 0.3%至 44.02 美元，Verizon 股价反而上升 1%至 52.39 美元。

6）英国电信运营商 CarphoneWarehouse 240 万用户个人信息泄露

法律依据：《数据保护法案》

案例描述：据《华尔街日报》杂志版 2015 年 8 月报道，英国电信运营商 Carphone Warehouse 表示，在近来备受外界关注的黑客入侵事件中，约有 240 万在线用户的个人信息遭到黑客入侵，包含姓名、地址、出生日期和加密的信用卡数据。根据《数据保护法案》规定：处理过程中应确保个人数据的安全采取合理的技术手段、组织措施，避免数据未经授权即被处理或遭到非法处理，避免数据发生意外毁损或灭失（“数据的完整性与保密性”）。控制者有责任遵守以上第 1 段，并且有责任对此提供证明。（“可问责性”）违反相关规定，英国信息专员办公室有权对违反该项数据法的公司施以高达 1700 万英镑(约合人民币 1.49 亿元)的罚款，或者征收该公司 4%的全球营业额。

1.3.3 数据使用风险

在数据使用环节，风险威胁来自于外部因素、内部因素、系统安全等。外部因素包括账户劫持、APT 攻击、身份伪装、认证失效、密钥丢失、漏洞攻击、木马注入等；内部因素包括内部人员、DBA 违规操作窃取、滥用、泄露数据等，如：

非授权访问敏感数据、非工作时间、工作场所访问核心业务表、高危指令操作；系统安全包括不严格的权限访问、多源异构数据集成中隐私泄露等。

(1)国内

1）湖南某银行257万条公民银行个人信息被泄露

执法机构：绵阳市公安局网络安全保卫支队

法律依据：《刑法》、《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》

案例描述：湖南某银行支行行长，出售自己的查询账号给中间商，再由中间商将账号卖给有银行关系的“出单渠道”团伙，再由另外一家银行的员工进入内网系统，大肆窃取个人信息，泄漏的个人信息包括征信报告、账户明细、余额等。2016年10月，绵阳警方破获公安部挂牌督办的“5·26侵犯公民个人信息案”，抓获包括银行管理层在内的犯罪团伙骨干分子15人、查获公民银行个人信息257万条、涉案资金230万元。根据最高人民法院、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》中规定，未经被收集者同意，将合法收集的公民个人信息向他人提供的，属于刑法规定的“提供公民个人信息”；第四条规定，违反国家有关规定，通过购买、收受、交换等方式获取公民个人信息，或者在履行职责、提供服务过程中收集公民个人信息的，属于刑法规定的“以其他方法非法获取公民个人信息”。根据《刑法》的相关规定：违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以

下有期徒刑，并处罚金。违反国家有关规定，将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的，依照前款的规定从重处罚。[12]

2）某物流公司 10 亿条用户信息数据被出售

案例描述：2019 年，暗网一位 ID“f666666”的用户开始兜售某物流公司 10 亿条快递数据，该用户表示售卖的数据为 2014 年下旬的数据，包括寄（收）件人姓名、电话、地址等信息，10 亿条数据已经过去重处理，数据重复率低于 20%，数据被该用户以 1 比特币打包出售。[13]

(2) 国外

1）伟易达被曝 480 万家长及儿童信息泄露来源

法律依据：《美国儿童网络隐私保护法 COPPA》

案例描述：2015 年，全球最大的婴幼儿及学前电子学习产品企业伟易达，被曝出其存在安全漏洞，致使数百万家长和儿童的数据曝光，包括家长注册账号使用的姓名、住址、邮件、密码等。 2018 年，美国联邦贸易委员会(FTC)宣布对伟易达(VTech)2015 年因安全漏洞导致数百万家长及孩子的数据泄露事件进行处罚，宣布处以 65 万美元的罚款。《美国儿童网络隐私保护法 COPPA》规定，运营者需建立并维护合理的措施以保护儿童个人信息的保密、安全和完整性。采取合作的措施保证仅向有能力保护儿童个人信息的保密、安全和完整性并为其提供保障的服务提供商和第三方披露儿童个人信息。

作为对照，我国《个人信息保护法》规定，个人信息处理者处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意。个人

信息处理者处理不满十四周岁未成年人个人信息的，应当制定专门的个人信息处理规则。发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人。

2）Zoom 超 50 万个 Zoom 账户泄露并在 Dark Web 出售

案例描述：2020 年 4 月，Zoom 被爆出漏洞，黑客通过凭据注入攻击收集，在 Dark Web 和黑客论坛上，出售超过 50 万个 Zoom 帐户，1 块钱可以买 7000 个。泄漏数据包括邮箱、密码以及个人会议链接和密钥，甚至许多还被免费赠送。另外，2020 年 11 月据美国联邦贸易委员会(FTC)，Zoom 将制定一项全面的安全计划，以解决该公司涉嫌欺诈和不公平行为的指控。FTC 的指控可以追溯到 2018 年 Zoom 的 Mac 桌面应用程序的更新，该程序秘密安装了 ZoomOpener 网络服务器，绕过 Safari 浏览器的安全措施，在没有提醒的情况下启动该应用程序。根据协议，Zoom 将在以后的每次违规行为中面临高达 43280 美元的罚款。

1.3.4 数据加工风险

在数据加工环节，泄露风险主要是由分类分级不当、数据脱敏质量较低、恶意篡改/误操作等情况所导致。

(1)国内

1）某集团 80 万用户数据被删除

案例描述：2017 年，因某为公司误操作导致某集团 80 万用户数据丢，此次故障影响面非常大，涉及到钦州、北海、防城港、桂林、梧州、贺州等地用户，属于重大通信事故。事故发生后，某集团已经发布声明承认故障影响，技术人员

也已经展开紧急维修。有消息称因为此次事故，某为公司已经被某集团处以5亿罚款，同时某集团已经展开全国范围的系统大排查，主要针对某技术公司第三方代维隐患问题。[14]

(2)国外

1）代码资源托管网站运维人员误删300G数据

案例描述：2017年，著名代码资源托管网站Gitlab.com的一位工程师在维护数据时不慎删除约300GB的数据。本次事故也影响到了约5000个项目，5000个评论和700个新用户账户。

1.3.5 数据传输风险

在数据传输环节，数据泄露主要包括网络攻击、传输泄露等风险。网络攻击包括DDoS攻击、APT攻击、通信流量劫持、中间人攻击、DNS欺骗和IP欺骗、泛洪攻击威胁等；传输泄露包括电磁泄漏或搭线窃听、传输协议漏洞、未授权身份人员登录系统、无线网安全薄弱等。

(1)国内

1）“瑞智华胜”涉嫌非法窃取用户信息30亿条

案号：（2019）浙0602刑初1143号

法律依据：《中华人民共和国刑法》第二百八十五条、第二十五条第一款、第二十七条、第六十七条第三款、第七十二条第一、三款；《中华人民共和国刑事诉讼法》第十五条、第二百零一条

司法机关：浙江省绍兴市越城区人民法院

案例描述：邢某于2013年5月在北京成立瑞智华胜。瑞智华胜通过邢某成立的其他关联公司与运营商签订精准广告营销协议，获取运营商服务器登录许可，并通过部署SD程序，从运营商服务器抓取采集网络用户的登录cookie数据，并将上述数据保存在运营商redis数据库中，利用研发的爬虫软件、加粉软件，远程访问redis数据库中的数据，非法登录网络用户的淘宝、某博等账号，进行强制加粉、订单爬取等行为，从中牟利。案发前，瑞智华胜发现淘宝网在调查订单被爬的情况，遂将服务器数据删除。经查，2018年4月17-18日期间，瑞智华胜爬取淘宝订单共计22万余条（浙江淘宝网络有限公司实际输出1万条），向指定加粉淘宝账号恶意加淘好友共计13.7万余个（浙江淘宝网络有限公司实际输出2万个）。最终判决被告人王某犯非法获取计算机信息系统数据罪，判处有期徒刑二年，缓刑二年六个月，并处罚金人民币六万元。[15]

(2) 国外

1）南非大规模数据泄露事件3160万份南非公民数据被泄漏

案例描述：2017年，南非史上规模最大的数据泄露事件——共有3160万份用户的个人资料被公之于众，连总统祖马和多位部长都未能幸免。泄漏信息包括身份号码、个人收入、年龄，甚至就业历史、公司董事身份、种族群体、婚姻状况、职业、雇主和家庭地址等敏感信息。此次被黑客公布的数据来源于 Dracore Data Sciences 企业的 GoVault 平台，其公司客户包括南非最大的金融信贷机构——TransUnion。

1.3.6 数据提供风险

在数据提供环节，风险威胁来自于政策因素、外部因素、内部因素等。政策因素主要指不合规的提供和共享；内部因素指缺乏数据拷贝的使用管控和终端审计、行为抵赖、数据发送错误、非授权隐私泄露/修改、第三方过失而造成数据泄露；外部因素指恶意程序入侵、病毒侵扰、网络宽带被盗用等情况。

(1)国内

1）脱口秀演员交易流水遭泄露，某银行被罚 450 万元

执法机构：中国银行保险监督管理委员会

法律依据：《中华人民共和国银行业监督管理法》第二十一条、第四十六条和相关审慎经营规则《中华人民共和国商业银行法》第七十三条

案例描述：2020 年 5 月 6 日，脱口秀演员池子（本名王越池）通过新浪微博控诉某银行上海虹口支行在未经其授权的情况下，私自将其个人账户流水提供给上海笑果文化传媒有限公司。王越池认为，某银行的这一行为侵犯了其合法权益，要求某银行赔偿损失，并公开道歉。同时，王越池还表示，某银行方面对此作出的回应为“配合大客户的要求”。对于举报，某银行也曾在官方微博公开发布致歉信称，该行员工未严格按规定办理，向笑果文化提供收款记录；某银行已按制度规定对相关员工予以处分，并对支行行长予以撤职。2021 年 3 月 19 日，银保监会消保局公布的罚单信息显示，某银行因涉及客户信息保护体制机制不健全、客户信息收集环节管理不规范等四项违法违规行为，被处罚款 450 万元。[16]

2）掉进短信链接“陷阱”被骗 3.6 万余元

法律依据：[2014]10 号《关于加强商业银行与第三方支付机构合作业务管理的通知》第三条规定，银发(2009)142 号《中国人民银行、中国银行业监督管理

委员会、公安部、国家工商总局关于加强银行卡安全管理预防和打击银行卡犯罪的通知》第二条第（六）项，《中华人民共和国合同法》第一百零七条

执法机构：河南省高级人民法院

案号：（2019）豫民申 6252 号、（2018）豫 0326 民初 2446 号

案例描述：2017 年 3 月 18-19 日，顾某收到“车辆违规未处理”短信，在点击链接后，其建行账户被开通天翼电子商务、易宝支付、苏宁易付宝、北京百付宝、快钱支付、美团大众点评、支付宝、财付通、电 e 宝、拉卡拉、上海盛付通、某易宝等十余个第三方快捷支付服务，并通过其中部分第三方支付平台连续扣款 52 笔，每笔金额从 1 元至 2500 元不等，共计 36960.79 元。顾某报警后，在公安机关和银行等机构的协作下，部分款项被追回并转入原告建行卡中，剩余 17728.94 元未能追回。法院认为，被告建行汝阳支行在为原告顾三斗办理银行卡时提供的相关格式文件条款中，未能反映出原告顾三斗主动申请并书面确认开通网上银行或电子银行等业务，原告因点击手机不明链接导致账户资金被盗取，较大可能系不法分子通过网上银行或电子银行操作，被告未能严格按照上述通知要求执行，对此应承担相应的责任。[17][18]

1.3.7 数据公开风险

在数据公开环节，泄露风险主要是很多数据在未经过严格保密审查、未进行泄密隐患风险评估，或者未意识到数据情报价值或涉及公民隐私的情况下随意发布的情况。

(1)国内

1）微信朋友圈中流传着某医院数千人名单

执法机构：胶州市公安局

法律依据：《中华人民共和国治安管理处罚法》第二十九条

案例描述：2020 年 4 月 13 日，微信群里出现某医院出入人员名单信息，内容涉及 6000 余人的姓名、住址、联系方式、身份证号码等个人身份信息，造成了不良社会影响。依据《中华人民共和国治安管理处罚法》第二十九条规定，有下列行为之一的，处 5 日以下拘留；情节较重的，处 5 日以上 10 日以下拘留：违反国家规定，对计算机信息系统中存储、处理、传输的数据和应用程序进行删除、修改、增加的。公安机关依法对叶某、姜某、张某给予行政拘留的处罚。[19]

2）邯郸市丛台区政府泄露特困人员隐私法律

执法机构：丛台区政府办公室

法律依据：《网络安全法》第 42 条、第 72 条

案例描述：2020 年 8 月 24 日，河北省邯郸市丛台区人民政府信息公开网站发布了一份《丛台区 2020 年 8 月份农村特困供养金发放明细》，公示了黄粱梦镇、三陵乡、兼庄乡、南吕固乡的 129 位村民的信息，公示名单中除了所属乡镇、姓名、发放款数、备注等信息之外，还悉数公开了村民的身份证号和银行卡号。经核实，发布机构丛台区民政局确实存在泄露隐私的问题，随后删除了该名单，并受到了内部公开群内通报批评，书面反馈整改内容的处罚。[20]

1.4 数据风险制约产业创新

据 IDC 预测，2025 年全球数据量将高达 175ZB。其中，中国数据量增速最为迅猛，预计 2025 年将增至 48.6ZB，占全球数据圈的 27.8％，平均每年的增长速

度比全球快3%，中国将成为全球最大的数据圈[1]。面对指数级增长的数据，数据共享流转、数据跨境流动、新技术演进、新业态出现等均会带来潜在伴生风险。因此，需要从国际国内大势出发，从内外部威胁梳理，从纵深演进分析数据安全面临的威胁和挑战，有助于倒逼技术产品创新升级，深化危机应对措施，化解重大风险挑战，保障数据安全。

1.4.1 数据跨境流动带来新隐患

随着全球数字经济的发展，数据跨境流动成为推动国际贸易中货物、服务、人、资金流动不可或缺的部分，并且在促进经济增长、提升创新能力、推动全球化等方面发挥着积极作用。然而，数据跨境流动的价值与风险越来越凸显，数据跨境流动风险与隐忧主要集中于数据的传输、存储和使用三个环节。传输上，数据跨境过程环节多、路径广、溯源难，传输过程中可能被中断，数据也面临被截获、篡改、伪造等风险；存储上，受限于数据跨域存储当地的防护水平等因素，容易出现数据泄露等问题；使用上，跨境数据的承载介质多样、呈现形态各异、应用广泛，数据所在国政策和法律存在差异、甚至冲突，导致数据所有和使用者权限模糊，数据应用开发存在数据被滥用和数据合规等风险。具体来看：

1、海量跨境数据难以梳理分类，不当应用引发风险隐患。一方面，数据在产生、存储后，被开放利用的情况随着数据采集、挖掘、分析等技术的不断发展而动态变化，加上数据体量大、增速快，当下未必就能准确地完成分级分类评估；另一方面，跨境流动中已被开发利用的各类数据，呈现形态各异、应用领域广泛、价值定义不明的状态，新技术、新业态引发的数据风险未知大于已知，加剧了数据跨境流动的安全隐患。

[1] 数据圈指被创建、采集或是复制的数据集合

2、跨境数据攻击升级，黑灰产加剧数据风险。一是攻击者从独立的黑客扩展到具有特定目标诉求的专业团体。例如，全球最大的SIM卡制造商金雅拓曾遭英美联合攻击，SIM卡密钥被盗取，用于解密、监控移动通信用户的语音等通讯数据。二是攻击对象从个人设备逐渐升级为各类泛在网络设备、终端和软硬件，甚至包括关键信息基础设施。比如，移动设备的GPS、麦克风、摄像头，移动通信的SIM卡、蜂窝基站、热点、蓝牙、Wi-Fi，以及广泛分布的物联网设备等。三是攻击方式随着技术发展不断演变升级，更加多样、隐蔽、智能。以人工智能为例，通过对数据的推理学习，会使数据去标识化、匿名化等安全保护措施无效。

1.4.2 新技术迭代催生更多风险

随着云计算、大数据、物联网、人工智能、5G等数字经济新技术的发展，数据安全技术与之深度融合。新兴技术伴生新风险，为安全防线带来“新口子”。比如：网络架构的变化中虚拟化、边缘化、能力开放、切片等技术给 5G 带来多种安全风险；人工智能培训数据污染会导致人工智能决策错误，即所谓的“数据中毒”；物联网设备的处理能力和内存通常较短，导致其缺乏强大的安全解决方案和加密协议保护免受威胁；云计算模式下，传输数据需要依赖网络，由于网络自身的缺陷和技术弊端，在出现非法操作的情况下，黑客更容易入侵网络导致数据泄露。

进一步分析，一方面，数据价值凸显引来更多的攻击者，而新兴技术的应用使得外部攻击面不断扩大，数据安全防御能力亟待提升。另一方面，在新兴技术应用与数据安全防护间寻找平衡。新兴技术本身安全方面的脆弱性，容易带来新安全问题并增加引入恶意攻击的风险。在数字化转型与新兴技术的融合中，数据

交互的维度和范围增加，业务提供的个性化和复杂性提升，导致更多设施面临网络攻击。

1.4.3 新业态出现激发潜在危机

近年来，我国新业态不断涌现，尤其在新冠肺炎疫情对全社会数字生存能力大考期间，进一步催化了数字经济加速发展，一大批新业态新模式进一步涌现出来。2020 年 7 月 15 日，国家发展和改革委等 13 部门联合印发了《关于支持新业态新模式健康发展 激活消费市场带动扩大就业的意见》，提出数字经济 15 种新业态新模式，即：融合化在线教育、互联网医疗、线上办公、数字化治理、产业平台化发展生态、传统企业数字化转型、“虚拟”产业园和产业集群、基于新技术的“无人经济”、培育新个人、微经济、多点执业、共享生活、共享生产、生产资料共享、数据要素流通等。目前，数据安全技术广泛运用于政务、金融、央企、农工商教医旅等领域，实现了数据安全与行业场景特点的融合应用。伴随新业态的出现，数据资源安全正面临严峻挑战。

数据基础设施频受攻击，数据丢失及泄露风险加大。数据交易中心、移动智能终端承载大量重要业务数据和用户个人信息，但数据资产没有进行全生命周期跟踪，资产使用规则执行不佳；与国家等保三级安全技术框架仍存在灾备建设、身份认证、访问控制、内容安全、安全运营等多方面差距。此外，近年来针对 IDC 的攻击日趋增加，侵犯数据安全的恶意应用、木马等日益增多，对用户隐私和财产安全构成极大隐患。

敏感个人信息泄漏成重灾区。融合化在线教育、互联网医疗、线上办公等，受益于科技进步和大数据、人工智能、语音识别、直播互动等技术应用，用户体

验及产品效果得到提升。由于此类场景中，数据包含患者姓名、年龄、电话等个人敏感信息，因此成为不法分子窥视的重要目标。应用渠道主要分为两类：PC端互联网门户网站和移动客户端软件下载渠道。新冠肺炎疫情爆发引发了网络钓鱼和恶意软件攻击的新潮流，由于下载渠道的多样性，以及渠道对移动客户端软件的管理、技术检测等手段不足，使得具有钓鱼目的、欺诈行为的移动客户端软件仿冒成为不法者的工具。

二、数据安全产业迎来发展机遇

2.1 实战合规共驱安全产业

2.1.1 数据安全面临国内外挑战

面向“十四五”时期，信息技术快速演进，数字经济蓬勃发展，数字产业化和产业数字化快速推进，海量数据资源汇聚融合、开发利用，数据要素倍增作用凸显，助推数据资源“势能”转换为数字化转型升级的“动能”，推动数据价值的正向发挥，但也带来了严峻的数据安全挑战。

放眼于国外，数据潜在价值的凸显，使得各国高度重视并围绕数据开展战略博弈，全球数据安全形势日益严峻；着眼于国内，高价值数据泄漏、个人信息滥用情况突出，新技术迭代衍生出新的风险，针对数据的攻击、窃取、劫持、滥用等手段不断推陈出新，经济、政治、社会等各领域面临巨大潜在影响。其背后凸显出的是：缺乏数据安全整体管控、忽视数据安全能力建设的产业现状。

2.1.2 安全需求被置于次要地位

实际调研证实，企业出现安全投入比例不足、安全建设滞后于业务功能建设等情况，源于数据安全需求被企业管理者放在“次要地位”。

安全需求不被重视可用两个角度来解释：一是数据安全的建设者与受益者不一致，符合“经济学的外部效应”理论，类似化工企业如果没有《环境保护法》等法律制约，在不考虑社会责任情况下，其最经济的选择是就地排污排废。数据安全亦然，比如泄漏了大量个人信息，最终受害者是广泛用户，而企业没有实质

损失，因此企业往往会忽视数据安全建设。二是管理者的行为遵从“前景理论”（Prospect Theory），意味着人对损失和获得的敏感程度是不同的，损失的痛苦要远远大于获得的快乐,映射到数据安全方面,管理者往往认为自己是幸运儿，数据泄露等风险不会发生在自己身上，所以赌一把“业务先行、安全滞后”。

2.1.3 强合规监管深化鞭子效力

数据安全已成为事关国家安全与经济社会发展的重大问题。近年来，国家高度重视安全建设，统筹发展和安全，推进行业数据安全保障能力提升，构建起坚实有力的安全法律屏障，形成了《网络安全法》《密码法》《数据安全法》《个人信息保护法》“四法共治”新局面，使得合规监管权责更鲜明、制度更健全、技术更创新。

“四法”之间紧密关联又各有侧重，《网络安全法》提出了安全治理道路，《数据安全法》和《个人信息保护法》明确了保护目标，提出了数据保护的“中国方案”，而《密码法》强调了保护信息与数据的技术手段。

结合顶层设计、法律法规，数据安全新监管同时体现对过程和结果的合规要求。数据处理者既应当从过程方面积极履行数据安全保护义务，也要对数据安全防护的最终结果负责。

2.2 数据安全成为国家战略

2.2.1 国际数据安全发展战略概况

数据安全是事关国家安全和发展、事关人们工作生活的重大战略问题，应该从国际国内大势出发，总体布局，统筹各方，创新发展。一个安全稳定繁荣的网

络空间，对各国乃至世界都具有重大意义。随着数据量呈指数级增长，数据安全成为美国、欧盟、英国等国家经济发展和国际竞争力提升的新引擎。大国竞争正在从国际规则制定权竞争向技术标准制定权转移。各国纷纷制定法律政策、技术标准，在数据安全领域进行国家战略博弈，以图占据价值链的制高点。

2.2.1.1 美国数据安全战略

2019 年 2 月美国发布《国防部云战略白皮书》，提出“国防部将安全从边界防御，转向聚焦保护数据和服务”。2020 年 1 月 1 日正式生效的美国《加利福尼亚州消费者隐私法案》，赋予消费者对公司收集和管理其个人信息更多的控制权，规范了企业收集处理数据的方式。2019 年 12 月，美国发布《联邦数据战略和 2020 年行动计划》，以 2020 年为起始点，规划了美国政府未来十年的数据愿景，核心思想是将数据作为战略资源来开发，通过确立一致的数据基础设施和标准实践来逐步建立强大的数据治理能力，为美国国家经济和安全提供保障。2020 年 10 月，美国发布《国防部数据战略》，提出其将加快向“以数据为中心”过渡，制定了数据战略框架，提出数据是战略资产、数据要集体管理、数据伦理、数据采集、数据访问和可用性、人工智能训练数据、数据适当目的、合规设计等八大原则和数据应当可见的、可访问的、易于理解的、可链接的、可信赖的、可互操作的、安全的等七大目标。

2.2.1.2 欧盟数据安全战略

2020 年 2 月，欧盟发布《欧盟数字化战略》《数据战略》《人工智能战略》，旨在建立欧盟数据平台的基础上，实现数据主权和技术主权，从而达到数字经济时代国家竞争力提升和领先。2020 年 6 月，德国和法国合作启动欧洲数据基础

架构 GAIA-X 项目，该项目被视为一个开放的数字生态系统摇篮，是欧洲国家、企业和公众联合建设的下一代数据基础设施。

2018 年 5 月，发布《通用数据保护条例》（GDPR），明确了个人数据定义及适用范围，确定了数据保护的合法性基础、数据主体权利、数据控制者义务、数据流通标准、数据救济和处罚等。依据 GDPR 有关规定，欧盟对个人数据出境进行了高水平保护，并认为 GDPR 应该成为世界的标杆，并在实施数据战略中，力推让世界向欧盟看齐。与此同时，GDPR 实际也是全球众多国家、地区制定数据保护条例的重要参考。

2.2.1.3 英国数据安全战略

2018 年 5 月 23 日，英国正式通过新修订的《数据保护法》，加强数据主体对其个人数据的控制权、加强数据控制者义务。在脱欧之后，英国政府于 2020 年 9 月发布了《国家数据战略》，着眼于利用现有优势，促进政府、企业、社会团体和个人更好地利用数据，推动数字行业和经济的增长，改善社会和公共服务，并努力使英国成为下一代数据驱动创新浪潮的领导者。该《战略》还阐述了数据有效利用的核心支柱，确保数据可用性、安全可靠性。

2.2.1.4 其他国家数据安全战略

日本作为信息化高度发达、拥有领先网络信息技术的国家，对数据安全高度重视。日本第一部《个人信息保护法》于 2005 年 4 月 1 日起施行。随着互联网技术的不断发展，2015 年进行了大幅修正，2017 年 5 月 30 日，2015 年日本《个人信息保护法》（Personal Information Protection Act ，“PIPA”）（修订稿）全面实施。该法比较符合成文法国家的常见体例，从总则、有关机构职责、个人

信息保护的规则、个人信息处理业者的义务、个人信息保护委员会、附则、罚则等七个方面规定了七章的内容。

德国联邦议院于2018年 4月27日通过《个人信息保护调整和施行法》，其中包含新的德国BDSG《联邦个人信息保护法》。在这部新的法案中，已实施40年的BDSG进行了大幅调整以符合欧盟GDPR《通用数据保护条例》。

新加坡作为全球金融中心之一，被誉为“世界上最安全的国家之一”。新加坡的安全，不仅在于人身安全，还在于对个人信息数据的保障。新加坡当局于2012年出台《个人数据保护法》后，为了更好的执行《个人数据保护法》，新加坡个人数据保护委员会出台了一系列条例及指引。其中条例包括2013年《个人数据保护（违法构成）条例》、2013年的《个人数据保护（禁止调用注册表）条例》、2014年的《个人数据保护（执行）条例》，上述三项条例与2014年的《个人数据保护条例》一起于2014年7月2日起实施。此外，还包括2015年1月23日开始实施的《个人数据保护（上诉）条例》。

印度于2018年下半年发布《个人数据保护法案》（PDP），一项综合性的个人数据保护法。该法案在欧盟GDPR颁布后做出了修改，同时，该法案已提交国会进行审议。该法案规定了个人数据采集、存储、处理和传输的方式。

泰国政府于2018年9月向国会提交了包含GDPR特色的个人数据保护法（PDPA）草案，2019年2月，泰国国会审议通过了该法案，并将于政府公报一年后（2020年5月下旬）开始施行，这也是泰国第一部规范私人数据采集、适用、披露的法律，具有极其重要的意义。

巴西于2018年8月通过第一部综合性的数据保护法，《The General Data Protection Law》(GDPL)。GDPL将依然受限于已经获得通过的近200条修正案，这些修正案关系到数据保护立法基础、公共主体数据保护法律适用以及数据安全的技术标准等实质问题。[1]

2.2.2 我国数据安全立法监管加强

近年来，国家陆续出台相关法律政策，统筹发展和安全，推动数据安全建设。《中共中央国务院关于构建更加完善的要素市场化配置体制机制的意见》明确要求加强数据安全。《中共中央关于制定国民经济和社会发展第十四个五年规划和二〇三五年远景目标的建议》明确提出：保障国家数据安全，加强个人信息保护。随着《国家安全法》《网络安全法》《密码法》《民法典》《数据安全法》《个人信息保护法》“五法一典”出台，我国数据安全法制化建设不断推进，监管体系不断完善，安全由“或有”变“刚需”。结合顶层设计、法律法规，数据安全新监管同时体现对过程和结果的合规要求。数据处理者既应当从过程方面积极履行数据安全保护义务，也要对数据安全防护的最终结果负责。

同时，我国强化数据安全技术自主创新，加速数据安全标准国际化进程。积极开展数据安全技术创新，提升产品性能，促进数据安全技术的成果转化；坚持立足于开放环境推进数据安全标准化工作，推进数据安全中国标准与国外标准之间的转化运用，扩大我国数据安全技术的国际影响力，进而鼓励数据安全企业进入海外市场，为交易流通、跨境传输和安全保护等数据安全应用的基础制度、标准规范和安全评估体系，保障跨境数据安全。（注：我国数据安全相关法律政策、技术标准详见附录.）

2.2.3 全球公正数据安全规则构建

开放合作是增强国际经贸活力的重要动力，并逐步变成国际合作主题。在全球经济贸易和产业分工合作日益密切的背景下，确保信息技术产品和服务的供应链安全对于提升用户信心、保护数据安全、促进数字经济发展至关重要。在全球范围构筑公正的数据安全规则成为主权国家重要诉求。

2020 年 9 月 8 日，中方发起《全球数据安全倡议》。该倡议是数字安全领域首个由国家发起的全球性倡议，聚焦全球数字安全治理领域核心问题，旨在通过明确政府行为规范、推动企业共担责任、合作应对安全风险等务实举措，为加强全球数字安全治理、促进数字经济可持续发展提出中国方案，贡献中国智慧。

2021 年 3 月 29 日，中国与阿拉伯国家联盟共同发表了《中阿数据合作与安全倡议》，阿拉伯国家成为全球范围内首个与中国共同发表数据安全倡议的地区。中阿在数字治理领域的高度共识，有利于推进数据安全领域国际规则制定，标志着发展中国家在携手推进全球数字治理方面迈出了重要一步。

2021 年 9 月 27 日，在 2021 世界互联网大会乌镇峰会网络安全技术发展和国际合作论坛上，与会专家一致认为，当前虚拟世界与现实世界高度融合趋势凸显，其“虚拟”特点易使网络空间边界和游戏规则被破坏。而网络攻防属于高对抗的领域，攻击手段不断推陈出新，在开放条件下带来的技术点多面广更需要协同。同时，网络安全涉及供应链、人员、经济、法律等多个方面，整体考虑需要资源优势互补，一旦出现问题将带来共同的利益受损，网络安全领域的多层面合作是最佳选择。

2.3 多重因素推动技术升级

数字时代背景下，一方面数据战略价值凸显，各国围绕数据展开战略竞争；另一方面数据成为安全重灾区，近年来针对数据的攻击、窃取、劫持、滥用等手段不断推陈出新，使得经济、政治、社会等各领域面临着巨大的风险。随着数字与现实世界的打通融合，数据安全的复杂度发生了质变，原有的对抗思路、技术储备、防护模式、建设路径等都陷入难以适应的被动局面。如何为数据安全建设注入“免疫力”，成为各领域数字化转型的关键。

2.3.1 数据安全攻防视角的新框架

2.3.1.1 传统“老三样”防御手段面临挑战

回顾过去，不难发现传统网络安全是以防火墙、杀毒软件和入侵检测等“老三样”为代表的安全产品体系为基础。传统边界安全防护的任务关键是把好门，这就好比古代战争的打法一样。在国与国、城与城之间的边界区域，建立一些防御工事，安全区域在以护城河、城墙为安全壁垒的区域内，外敌入侵会很“配合”地选择同样的防御线路进行攻击，需要攻克守方事先建好的层层壁垒，才能最终拿下城池。其全程主要用力点是放在客观存在的物理边界上的，防火墙、杀毒软件、IDS、IPS、DLP、WAF、EPP 等设备功能作用亦如此。

而观当下，云计算、移动互联网、物联网、大数据等新技术蓬勃发展，数据高效共享、远程访问、云端共享，原有的安全边界被“打破”了，这意味着传统边界式防护失效和无边界时代的来临。

2.3.1.2 由应对到主动的安全防护技术升级

IT 系统不可避免的存在缺陷，利用缺陷进行漏洞攻击或是网络安全永远的命题，攻防对抗视角的网络安全防护是过去主要的安全防护手段。当然，所有网络安全防护最终还是为了保护数据，防止“偷数据、改数据”，但是今天我们认为网络漏洞始终在所难免，所以需要从“防漏洞、补漏洞”的应对式防护，转化到“为数据访问重建安全规则”的主动式防护，也即“以数据为中心的安全”，这也是安全技术不断进化的必然产物。

在实践中，需要把“以网络攻防为中心的安全”和“以数据保护为中心的安全”相结合，两者相辅相成、齐驱并进，方可全方位保护网络与数据生命周期安全。

2.3.1.3 大数据时代下数据安全防护挑战空前

大数据时代，数据的产生、流通和应用变得空前密集。分布式计算存储架构、数据深度发掘及可视化等新型技术、需求和应用场景大大提升了数据资源的存储规模和处理能力，也给安全防护工作带来了巨大的挑战。

首先，系统安全边界模糊或引入的更多未知漏洞，分布式节点之间和大数据相关组件之间的通信安全薄弱性明显。

其次，分布式数据资源池汇集大量用户数据，用户数据隔离困难，网络与数据安全技术需齐驱并进，两手同时抓。突破传统基于安全边界的防护策略，从防御纵深上实现更细粒度的安全访问控制，提升加密算法能力和密钥管理能力，是保证数据安全的关键举措。

再次，各方对数据资源的存储与使用的需求持续猛增，数据被广泛收集并共享开放，多方数据汇聚后的分析利用价值被越来越重视，甚至已成为许多组织或

单位的核心资产。随之而来的安全防护及个人信息保护需求愈发突出，实现“数据可用不可见、身份可算不可识”是重大命题，也是市场机遇。

最后，数字化生活、智慧城市、工业大数据等新技术新业务新领域创造出多样的数据应用场景，使得数据安全防护实际情境更为复杂多变。使得如何保护数据的机密性、完整性、可用性、可信性、安全性等问题更加突出和关键。

2.3.1.4 建设以数据为中心的安全治理体系

对国家而言，致力构建与时俱进的网络空间数据安全保障体系，努力实现从应对到主动防护的战略转变，以维护国家网络空间安全，是事关国家安全和人民利益；事关服务关键信息基础设施和重要信息系统安全可控的国家战略需求。

对企业或组织而言，数据安全治理是事关自身资产安全、可持续发展战略的必经之路，须从保护商业秘密、业务安全、客户权益等方面扎实做好数据安全防护工作。一是保护数据本身安全，即数据机密性、完整性、可用性；二是满足国家相关法律法规对个人信息和关基的合规性要求。

这就决定，数据安全防护需以“数据为中心”建立安全防护与治理体系，聚焦数据与生态，明确数据的使用、存储、传输场景，构建由数据安全组织管理、合规治理、技术防护“三部曲”组成的覆盖数据全生命周期的防护与治理体系。

2.3.2 数据安全供需市场的新博弈

2.3.2.1 宏观看市场角色转变

传统的网络与信息安全市场，需求潜力巨大、但供给相对不足，所以看似是甲方市场，实际上是乙方市场。一方面，甲方对市场定价，掌握安全产品、安全

服务价格话语权，表面是甲方在主导市场。但另一方面，整个市场技术发展和水平，主要由乙方主导。

在数据时代，在实现对数据本身客观保护时，要解决数据与业务的高度纠缠问题，可以说数据安全天生带着深刻的业务适用属性，如果脱离业务场景，不可能实施数据的有效保护，所以数据安全技术与产品，需要在丰富业务场景中持续迭代和验证。基于以上考虑，甲方需要亦可能成为数据安全市场主导者。

2.3.2.2 中观看产业定位转变

传统的网络与信息安全行业，主要呈现通用安全技术和手段覆盖，整体的产品体系是“硬件-软件-服务”格局。上游：网络安全产业链上游为基础硬件提供商，为中游设备厂商提供芯片、内存等基础元器件；中游：产业链中游主要是安全硬件设备厂商、安全软件厂商和安全集成厂商；下游：产业链下游主要为各类用户主要为政企客户， 包括政府、军工、电信、教育、金融、能源等。

数据安全时代，在宏观市场供给与需求双方角色切换下，传统下游将掌握更大话语权，能整合上下游资源的企业将获得更高效的运作效率。产业链下游企事业单位为了实现安全目标或定制化需求，同时在全球化竞争格局新变化形态下，有可能进行中游乃至上游的关键产业链环节整合，比如新型物联网企业可能整合安全芯片、安全固件、安全服务器、安全中间件以及安全方案集成全产业链整合或资源优化。

2.3.2.3 微观看技术实现转变

传统的网络与信息安全技术，侧重于对硬件或软件加固，或侧重于通用的网络流量解析和攻击特征分析，结合身份认证体系，最终实现业务完整性和可用性、

数据机密性以及内容合规性。而数据安全威胁作为复杂业务处理的伴生风险问题，通用的传统安全技术难以直接照搬，数据安全要求安全能力作用于业务流和数据本身，而企业不同的业务形态要求贴身的保护手段。

针对数据本身或者结合数据内容表达上下文特征，建立数据生命周期保护是实施数据安全保护的主要手段。同时，针对海量的数据资产或关联数据，往往需要在业务场景中运用大数据分析、AI 算法。同时，数据安全所涉及的前沿技术本身需要政企客户自身业务和数据模型支持。

2.3.3 数据安全实战能力的新要求

2.3.3.1 数据安全要侧重数据保护能力

从数据安全技术转变，可以看出数据安全更加侧重要数据保护能力（传统网络安全主要为检测响应）。在数据集约化、规模化发展前，受限于 IT 技术和产业发展影响，数据留存与分析本身不是 IT 建设重点（主要是业务实现）。进而，对数据自身保护往往有限，比如大量数据明文存储（2011 年，CSDN 账号口令被拖库可以看出，敏感数据保护是常见短板）；再比如企业重要文件无异地备份（2014 年，勒索病毒爆发后，较多企事业单位敏感文件无法找回）。

当前，在国家法律法规持续完善的合规引导下，企事业单位应当建立主动的数据保护体系，在数据安全管理制度下，从数据本身内容表达进行机密性、可用性、完整性、价值、使用价值、属主等关键要求保护。

2.3.3.2 数据安全要赋能业务运营能力

传统的网络安全、信息安全技术手段，往往不考虑业务特性，侧重于信息化

系统，通过点式防护，堆积可复制化设备来实现安全。然而，数据是业务组织经营和业务运营的关键因子。企业保护数据要求结合组织使命和业务特征，实现场景化的解决方案。比如，业务要求实现对互联网用户提供消费服务，那么，管理者需要考虑用户敏感个人信息存储安全、展示安全，需要考虑结合业务数据和个人信息互联网传输安全，本质上要求管理者把数据安全能力赋予组织业务运营。

2.3.3.3 数据安全要提供服务支撑能力

云服务、数据中心成为数字经济时代关键信息基础设施之一，成为企事业单位优化 IT 架构最主要实施手段。进而，数据安全亦要成为服务于信息化重要支撑。在满足监管合规要求的前提下，数据安全能力建设要契合业务发展需要（以数据治理为中心的业务运营理论将成为主要组织目标），同时应结合管理、技术、运营形成服务能力，为组织持续的数据增长、业务发展提供长久保障。结合业务场景，通过数据资产管控技术，建立面向统一数据调度方式，形成良性数据共享机制，提高数据置信度、优化模型合理性、数据流转更清晰，管理权责更明确，在以成效为导向的价值标准下，数据安全服务支撑能力成为组织数据安全能力建设核心之一。

2.3.4 数据安全思路模型的新演进

在全球贸易形态新变化和后疫情时代下，数据安全面临的安全风险与挑战越来越复杂。基于此，实现数据安全通常有两种思路。第一种思路是复杂对抗复杂，建设复杂管控平台，在数据全生命周期流转的各个环节，发现数据安全威胁，加固数据安全漏洞；第二种思路是安全思路与模型的进化，即在网络安全“防漏洞，堵漏洞”思路的基础上，结合数据安全侧重要于保护思路，进行新安全模型进化

[2]。

进一步探索，传统的网络安全经典模型是 DR（检测/响应）模型，并进行不断完善如 PDR（防护/检测/响应）、P2DR2（策略/防护/检测/响应/恢复）模型等。其特征是，其中 PDR 安全模型是基于时间的动态安全模型，如果信息系统的防御机制能抵御入侵时间，能超过检测机制发现入侵的时间和响应机制有效应对入侵时间之和，那么这个系统就能有安全保障。然而，在数字时代，5G、物联网、云服务等技术大量应用，入侵检测时间和响应机制不足满足数据和数据价值保护时间。

而对于数据安全新思路和新模型，则是在对数据的防护能力顺序、空间颗粒度、数据状态等多个维度上，采用面向失效的安全理念，协同联动的叠加多种安全保护机制。故本文重点考虑了在数据安全实现中的新思路和新安全模型。

[2]本文章侧重于第二种思路，即模型与思路的安全进化。

三、数据安全技术亟待叠加演进

3.1 数据安全需要新框架

数据的最大特征就是流动，只有流动中的数据才能创造价值。对于重要信息系统而言，软硬件漏洞不可避免，未知威胁层出不穷，内外夹击形势严峻，传统的防御思路已不能有效应对，与其陷入无休止地“挖漏洞、补漏洞”的被动局面，不如寻求数据防护的新思路，探索数据安全建设新框架。

3.1.1 数据安全需兼顾内外威胁防护

数据安全面临的风险主要来自两方面。一是带有获利目的的外部威胁与对抗的持续升级，加之新兴技术演进带来不可预知的安全风险。二是来自内部的安全风险，即传统安全体系存在着固有的问题。

针对外部数据安全威胁，Canalys《网络安全的下一步》报告显示，2020 年数据泄露呈现爆炸式增长，短短 12 个月内泄露的记录比过去 15 年的总和还多。其中，最为明显的特征是勒索软件攻击激增，相比 2019 年增长了 60%，成为主要数据泄露渠道。

针对内部安全风险，传统的网络安全设备注重单点防护、静态防护，缺乏联动能力，且对未知威胁缺乏“看得见”的能力。同时，安全管理系统往往存在重建设、轻运营，缺乏有效的安全运营工具和手段，难以定位攻击方，缺乏事后分析、追溯能力等不足。

网络和数据安全始终是攻击者和防御者之间的战斗。未来具有不确定性，但能肯定的一点是：作为数据安全的防御者，仍将继续面临新的、不断演化的网络安全威胁与挑战。

3.1.2 数据防护从应对式转向主动式

然而，目前的数据防护主流思路是应对式防御，通常是系统遭受了攻击后，根据攻击情况采取行动，包括且不限于：传统杀毒软件、基于特征库入侵检测、病毒查杀、访问控制、数据加密等手段，“滞后于攻击手段”的弊端明显。传统“封堵查杀”难以适应时代发展，应对拟人化和精密化的攻击，且容易被攻击者快速发现漏洞，针对薄弱点进行精准攻击，不利于整体安全。

当下来看，网络漏洞始终在所难免，应对式防御“治标不治本”，直接针对数据本身进行主动式防护，是实现数据安全的最直接有效的手段，这也是“以数据为中心的安全”。

构建主动防护能力，政策已先行。于 2019 年 12 月 1 日起正式实行的等保 2.0 标准，在 1.0 时代标准的基础上，也更加注重主动防御，从被动防御到事前、事中、事后全流程的安全可信、动态感知和全面审计，不仅实现了对传统信息系统、基础信息网络的等级保护，还实现了对云计算、大数据、物联网、移动互联网和工业控制信息系统的等级保护对象的全覆盖。

对于行业来说，威胁和安全响应就是一场时间赛跑，以主动式防护为代表的产品和服务需求未来必将快速增长。主动式防护将实现安全运营、安全态势感知

与防御协同形成联动，能够在面临威胁时做到从容不迫，并给予“道高一丈”式压制打击。

3.1.3 网络与数据并重的新建设思路

传统的城防式数据安全，主要是保护被传统物理网络多层包围的数据，这种防护体系仅适用于保护静态数据。但当下，数据已成为新生产要素，数据被充分共享流转以产生价值，传统城防式数据安全已经难以满足需求。

我们认为，数据与“网络/主机/数据库/应用”是正交关系，“以数据为中心的安全”本质，是在数据流转的多个层次环节中，通过重建业务规则，对数据施加主动式安全防护，即直接对数据本身进行加密、访问控制、安全审计等安全手段。结合企业信息化发展，以数据为中心的安全建设理念是更加有效的做法。

以网络为中心的安全体系是保证数据安全的前提和基石，而以数据为中心的安全，以数据为抓手实施安全保护，能够更有效增强对数据本身的防护能力。因此，网络与数据并重的安全建设成为大势所趋。“以网络攻防为中心的安全”与“以数据保护为中心的安全”之间是相互关联、彼此依赖、叠加演进的。

图 1 网络与数据并重的新安全建设理念

着眼当下，数据安全所面临的问题不是做的过多导致冗余，而是出血口太多、防护能力达不到。事实上，应用系统、安全产品、基础设施都潜藏着漏洞，或者存在考虑不周的安全设计缺陷。好的安全理念应该是以网络与数据并重为新建设方向，面向失效的安全机制，通过有联动协同的纵深安全机制，构建有效防线。

从针对数据本身进行主动式防护出发，将数据安全技术组合赋能给具体行业安全问题，比发掘一个适用于所有行业的通用问题，更符合用户的实际需求。在数据安全建设的发展进程中，不断洞悉时代发展需求，创造性地提供新框架、新方法，能够有效带动其他参与者在一个良性的生态中协同共进，为数据安全建设带来全新突破。

3.1.4 经典网络安全框架 ATT&CK

作为网络安全行业目前公认权威、并被普遍接受的网络攻击模型框架，ATT&CK 是由 MITRE 公开发布于 2015 年，全称是 Adversarial Tactics，Techniques, and Common Knowledge（对抗性的战术、技术和通用知识）。从最初的一个内部

人员分享的 Excel 电子表格工具，到如今已经发展成为威胁活动、技术和模型的全球知识库，ATT&CK 汇聚来自全球安全社区贡献的基于历史实战的高级威胁攻击战术、技术，形成了针对黑客行为描述及相应防御构建的通用语言和知识图谱，并在企业、政府和安全厂商中广为流行。

目前，ATT&CK 当前主流版本包括 14 个攻击战术、205 个攻击技术、573 个攻击流程，覆盖了绝大多数网络攻击手段，使安全运营不仅知己而且知彼，从而有机会衡量安全体系应对攻击的纵深防御、检测响应能力，并在实战对抗中持续改进提升，能够为网络安全防护提供专业的技术参考。ATT&CK 框架以及关联的 Shield 主动防御框架，以网络攻防为视角，侧重“以网络为中心的安全”保护思路，通过“防漏洞、堵漏洞”的方式保护数据。

3.1.5 数据安全技术框架 DTTACK

进入数据时代，侧重攻防对抗的 ATT&CK 框架，难以覆盖“主动式保护数据”的各种技术手段。炼石尝试从“以数据为中心”的角度提出 DTTACK 数据安全技术框架，全称是 Data-centric Tactics, Techniques And Common Knowledge（以数据为中心的战术、技术和通用知识）。

3.1.5.1 DTTACK 的设计思路

网络安全持续的变化，攻防之间的博弈在不停的进化，已有的网络安全能力的度量逐步显露出局限性和不适用性。数据安全建设领域亟待出现新的安全能力度量方式，以应对不断变化的网络与数据安全发展趋势。

如果说 ATT&CK 的出现，是让攻击手法拥有通用语言，那么 DTTACK 的诞生便是对数据本身进行主动式防护，为防护模式打造了通用技术库。DTTACK 不是网络服务器或应用程序安全性的模型，它更强调数据本身的安全性，并从对数据的应对式防护向主动式防护转变，重视从业务风险映射视角列举数据保护需求，也可以为信息化建设、企业业务架构设计提供数据安全能力参考。

目前，炼石已初步梳理 6 个战术，31 个技术，83 个扩展技术，145 个方法，并持续更新迭代，致力于打造数据安全领域的专业权威技术框架。

3.1.5.2 DTTACK 的设计理念

DTTACK 框架列举了诸多技术，其作用类似于“兵器库”，防守方需要体系化的思路整合这些技术，才能利用好先发优势，精心“排兵布阵”，环环相扣构造纵深防御战线，体系化的防范内外部威胁，提升防御有效性。

（1） 重视从业务风险映射视角列举数据保护需求

安全本质上是一种业务需求，“传统业务需求”侧重于“希望发生什么”，而“安全需求”侧重于“不希望发生什么”，从而确保“发生什么”。从这个角度看，各种安全的定义都可以映射到业务需求，比如 Security（安全防攻击）、Safety（安全可靠）、Reliability（可靠性）、Trustiness（诚信度）以及 Sureness（确定性）等。而数据安全需求重点是数据的机密性和完整性。

当前版本的 DTTACK，在数据安全技术列举方面，参考了工信部相关机构正在编制的行业标准《电信网和互联网数据安全管控平台技术要求和测试方法》，将 114 个具体技术流程分类并对号入座，为数据安全建设提供技术支持。

（2） 结合 NIST 安全能力模型、安全滑动标尺模型

DTTACK 框架的构建，以 NIST 安全能力模型和安全滑动标尺模型为参考，并做了整合与精简。基于此，DTTACK 最新版本选择了六大战术作为基本结构：IDENTIFY（识别）、PROTECT（防护）、DETECT（检测）、RESPOND（响应）、RECOVER（恢复）、COUNTER（反制）。

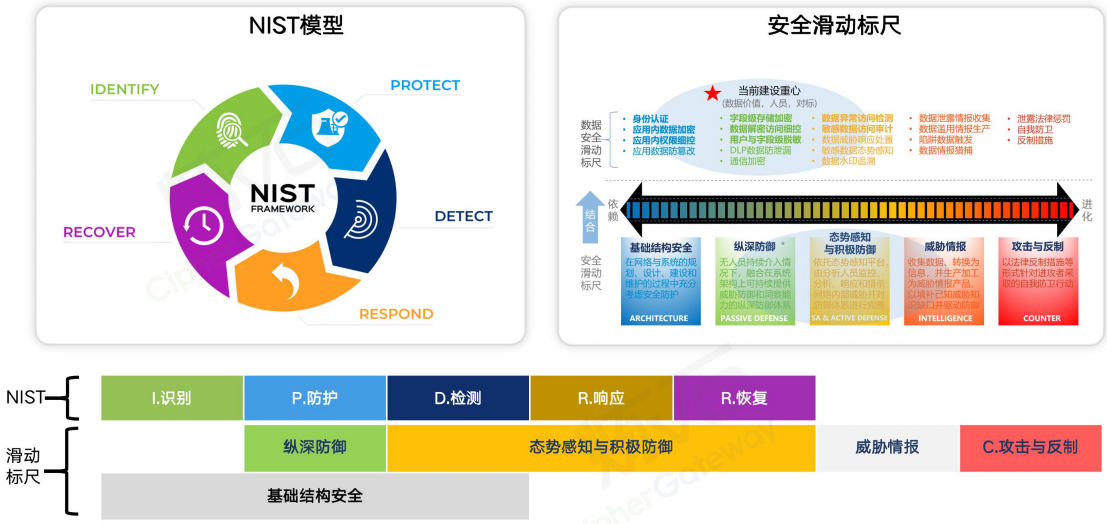

图 2 参考 IPDR2 和安全滑动标尺模型的结构

NIST CSF 是由美国国家标准与技术研究所（National Institute of Standards and Technology，简称 NIST）制定的网络安全框架（Cybersecurity Framework，简称 CSF），旨在为寻求加强网络安全防御的组织提供指导，目前已成为全球认可的权威安全评估体系。该体系由标准、指南和管理网络安全相关风险的最佳实践三部分组成，其核心内容可以概括为经典的 IPDRR 能力模型，即风险识别能力（Identify）、安全防御能力（Protect）、安全检测能力（Detect）、安全响应能力（Response）和安全恢复能力（Recovery）五大能力，实现了网络安全“事前、事中、事后”的全过程覆盖，可以主动识别、预防、发现、响应安全风险。

安全滑动标尺模型为企业在威胁防御方面的措施、能力以及所做的资源投资进行分类，可作为了解数据安全措施的框架。模型的标尺用途广泛，如向非技术人员解释安全技术事宜，对资源和各项技能投资进行优先级排序和追踪、评估安全态势以及确保事件根本原因分析准确无误。该模型包含五大类别：基础结构安全、纵深防御、态势感知与积极防御、威胁情报、攻击与反制。这五大类是一个非割裂的连续体，从左到右，具有一种明确的演进关系，左侧是右侧的基础，如果没有左侧基础结构安全和纵深防御能力的建设,在实际中也很难实现右侧的能力有效发挥。从左到右，是逐步应对更高级网络威胁的过程。

深入研究发现，NIST 安全能力模型、安全滑动标尺模型两者有交集、但也各有侧重。DTTACK 融合两大模型中的丰富安全能力，并施加到流转的数据上，为防御纵深夯实技术基础，是提升数据安全建设有效性的关键之举。

（3） 发挥以密码技术为核心的数据安全实战价值

在 DTTACK 六大战术中，密码技术也为其提供了重要价值。比如：识别方面，密码可以为数据识别提供身份安全能力，为接口通道实现安全加密；防护方面，数据加密技术本身就是在开放式信道中，构建了强制的防护措施，并结合身份实现访问控制。检测、响应、恢复和反制方面，密码也能够为其分别提供身份鉴别、数据保护、水印追溯等不同能力。

尤其对于流转数据防护，密码技术可以提供独特价值。共享流转的数据很难有边界，在做访问控制的时候，如果数据库或归档备份中的数据是明文，访问控制机制很容易被绕过。而通过数据加密技术，可以打造一个强防护场景，用户在正常访问应用的过程中数据才会解密，并结合身份访问控制、审计等安全技术，

从而实现了“防绕过的访问控制”、以及“高置信度的审计”。密码技术为数据重新定义了虚拟的“防护边界”，从而更好地对数据实施防护与管控。

（4） 填补“以数据为中心”的安全技术体系空白

当下，数据已成为新生产要素，数据被充分共享流转以产生价值。凡是有数据流转的业务场景，都会有数据安全的需求产生。“以数据为中心”的安全强调数据处于中心位置，就需要站在数据的视角，纵观数据的生命周期，然后针对数据流转的每个关键环节重新审视安全问题和解法。

结合到企业或机构的信息系统中，数据安全则来自于业务处理中的风险映射。从时间维度看，数据在流转的全生命周期中的每个环节都会有相应的安全需求；从空间维度看，数据在基础设施层、平台层以及应用层之间流转，不同层次会有不同颗粒度的防护需求。

DTTACK 以数据安全领域的全地图技术框架为目标，可为不同场景的数据安全防护提供基本思路，期望在一定程度上助力提升全社会、全行业的数据安全水位，填补“以数据为中心”的安全技术体系的空白，为数据安全厂商提供通用知识库，为甲方的数据安全规划和技术对比提供参考依据。

3.1.6 网络与数据一体化的叠加演进

实际上，DTTACK 不是孤立的。由于“以网络攻防为中心的安全”与“以数据保护为中心的安全”之间是相互关联、依赖、叠加演进的，网络安全是实现数据安全的基础，但光靠网络安全又很难有效保护数据，数据安全新框架是安全技术演进的必然。因此，把“以网络攻防为中心的 ATT&CK 框架”和“以数据保护

为中心的 DTTACK 框架”相结合，两者相辅相成，将实现全方位多维度的网络与数据安全防护。

3.2 数据安全需要新战法

安全漏洞层出不穷，攻击手段与利用手法日益复杂精妙，攻击方和内部威胁方天然具有单点突破的优势。同时，在构建安全防御体系的过程中，由于防护规则覆盖难以面面俱到，或在具体实施过程中难免疏漏，或内部人员天然有接触数据的风险，这些都可能导致某个安全节点被突破失效，所以简单堆叠防护技术和产品在体系化进攻和日益复杂的内部威胁面前是难以奏效的。

面对数倍于防护速度的安全威胁，防守者需要摒弃“一招制敌”的幻想，体系化地与进攻者对抗，打造更为先进的防护战法，才能有效应对日益严峻的安全形势。基于 DTTACK 的防御纵深，将凭借强大的知识库和技术支撑，形成层层递进、协同联动的新战法，实现在网安对抗中的技高一筹。

3.2.1 知彼：攻击体系化

当下，数据安全防御变得越来越困难，各种强悍的防御手段，在一些“精妙”的攻击下都很快被击破，比如 APT 攻击让传统防御手段变得形同虚设，信息交互的刚需使网络隔离难以奏效，各种宣称“解决一起安全问题”的防御技术很快被绕过。究其根本，是伴随着安全体系建设的演进，攻击也呈现出体系化的发展趋势。

从攻击对象来看，只要有利益、有价值的系统和服务，都存在被攻击的现象，尤其是有影响力国家级、企业级数据，由于针对安全攻击能够带来高回报率，引来越来越多的活跃数据安全攻击团伙的全面研究与精准打击。

从攻击特点来看，攻击正变得更为聪明和大胆，不仅是蓄意且具备高智力的，而且逐渐向拟人化和精密化的方向发展。攻击者们不仅能够通过快速查明防御系统或环境中存在的漏洞，精确针对特定薄弱区域定制并发起大规模攻击，还能模拟合法行为模式以绕开和躲避安全工具。

从攻击趋势来看，过去针对数据安全漏洞层出不穷的情况，攻击手法大多都是“单点突破”，但绝大多数的单点突破，难以达到攻击目的。因此，攻击趋势正从“单点突破”向“体系化”转变，攻击手段也越来越专业，甚至攻击任务都出现了“黑产链”、“专业外包”等情况。在这样复杂的进攻下，传统的安全边界或网络隔离策略变得形同虚设。

当然，体系化的攻击也并非没有弱点。攻击的目的是获利，获利往往会让攻击暴露更多细节。在分析窃取信息为目的的攻击并设计防御措施时，特别需要关注“窃取”这个获利环节。定位寻找有价值的信息，读取访问获得目标信息，以及各种渠道回传窃取的信息，从而实现攻击的目的。如果没有获利环节，一次针对信息系统的攻击可能是没有效益的。另一方面，在整个攻击过程中，获利环节的隐匿性可能是最低的，而且由于攻击产业链的信任关系问题，其执行水平可能也是最差的。

3.2.2 知己：银弹不存在

可以看到，攻击者已经联合起来，形成分工合作的生态圈，如果防守依然处于孤立、静态且不成体系的，那么成功者毋庸置疑会是攻击者。基于分析，值得庆幸的一点是，攻击行为的体系化、链条化，恰恰带来了更多的防御点。

防御者首先要达成一个共识，数据安全建设不存在“银弹”，要放弃一招制敌的幻想。“银弹”即银色子弹，在欧洲民间传说及19世纪以来哥特小说风潮的影响下，往往被描绘成具有驱魔功效的武器，是针对狼人等超自然怪物的特效武器。用在数据安全建设领域，代表具有极端有效性的解决方法。但实际上，安全防护不可能达到 100% 的安全,即使是 1% 的漏洞,也可能造成 100% 的损伤。

数据依托于信息系统而存在，数据安全不仅仅局限于数据本身，而应扩展到信息系统的各安全领域。多层面、全方位、环环相扣的纵深防御，是目前保障数据安全的有效路径。

纵深防御（Defence in depth）概念来源于一种军事战略，在军事领域中是指利于纵深、梯次地部署兵力兵器，抗击敌人大纵深、立体攻击；利于疏散配置兵力兵器，减少敌方火力杀伤；利于实施兵力、火力机动，适时以攻势行动歼灭突入、迂回、机降之敌；利于组织指挥各部队、分队相互支援。数据安全领域的纵深防御是指，在信息系统上根据不同的安全威胁或系统攻击，结合不同的安全防护技术与措施，实施多层的安全控制策略，目标是提供了环环相扣、协同联动的安全防御，也意味着一种安全措施失效或被攻破后，还有另一种安全防御来阻止进一步的威胁，降低攻击者进攻成功的机率。

麻烦是永远存在的，除非主动解决，否则它不会主动消失。在数据安全建设领域也是这样，数据安全是件极其复杂的事，现在考虑进来的麻烦多了，未来遇到的麻烦就会少。事后消补永远不及设计之初就纳入安全，不论是效果还是成本都会有所体现。

3.2.3 百战不殆：面向失效的安全设计

知己知彼，才能百战不殆。针对数据安全漏洞的攻击变得体系化加大了防御的难度，但获利环节让攻击暴露更多细节，使得防御者有了更加精准的防护切入点。在数据安全防护过程中，不存在一招制敌的战法，基于 DTTACK 的防御纵深，将凭借先发优势、面向失效的设计、环环相扣的递进式设防，成为百战不殆的有效战术。

3.2.3.1 先发优势

为了对抗体系化的攻击，防御体系的设计应用好“先发优势”，针对威胁行为模式，提前布置好层层防线，综合利用多样化的手段，实现各个维度防御手段的纵深覆盖，让进攻者在防守者布局的环境中“挣扎”。

一方面，通过“排兵布阵”制定策略，结合 IT 基础设施、网络结构、系统分区、业务架构、数据流向等进行精心防御设计，消耗进攻者的资源；另一方面，是形成多道防线，每一道防线都是针对前一道防线破防的情形打造，而不是盲目的堆砌，这就需要提到面向失效的设计原则。

3.2.3.2 面向失效的设计

面向失效的设计原则是指，任何东西都可能失效，且随时失效。需要考虑如前面一道防御机制失效了，后面一道防御机制如何补上后手等问题，考虑系统所有可能发生故障或不可用的情形，并假设这些可能都会发生，倒逼自己设计出足够健壮的系统。是一种在悲观假设前提下，采取积极乐观的应对措施。

面向失效的设计是防御纵深的关键。整体思路：从传统静态、等待银弹的方式转向积极体系化的防御纵深模式。分析进攻者的进入路径，基于面向失效的设计原则，打造多样化多层次递进式的防御“后手”。

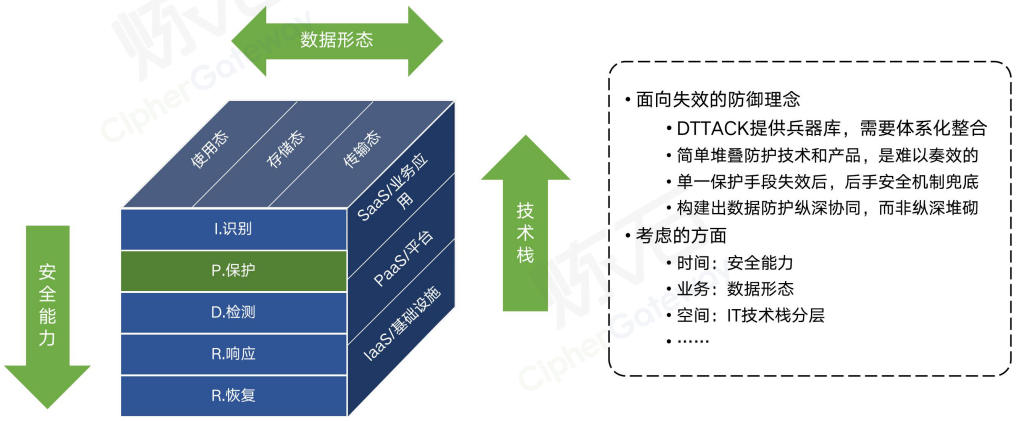

图 3 面向失效的数据安全纵深防御新战法

基于面向失效（Design for Failure）的防御理念，从几个重要维度层层切入，综合利用多样化手段构建纵深，当一种保护手段失效后，有后手安全机制兜底，打造纵深协同、而非简单堆叠的新战法。这里选择三个比较重要的维度，一是安全能力维度（I.识别、P.防护、D.检测、R.响应、R.恢复、C.反制），二是数据形态维度（使用态、存储态和传输态等），三是技术栈维度（SaaS/业务应用、Paas/平台、IaaS/基础设施），这三个维度之间关系是独立的、正交的，三者叠加可构建更有效的数据纵深防御体系。

3.2.3.3 数据安全纵深防御

“纵深防御”是一种应该体现在数据安全防御体系设计各个方面的基本原则，而不是一种“可以独立堆叠形成的解决方案”。

（1） 多层堆叠不等于防御纵深

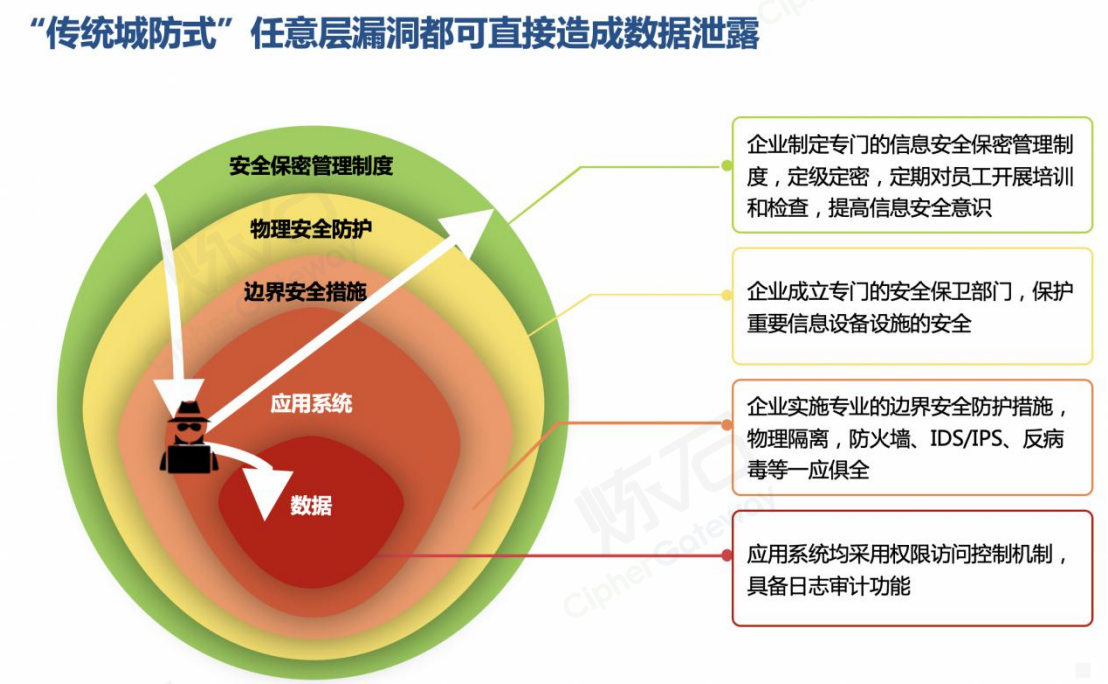

图 4 数据安全防护架构图

企业传统的城防式安全防护是将数据一层层地保护在中心，为了保护核心数据，在多个层面进行控制和防御，比如安全制度建设（安全意识培训）、物理安全防护（服务器加锁，安保措施等）、边界安全措施（使用防火墙等）、应用安全系统防御（访问控制、日志审计等）以及对数据本身的保护（数据加密等）。实际上任意层漏洞都可能直接造成数据的泄漏，导致之前建设的所有的安全手段就会瞬间瓦解。

例如，在2017年11月15日，Oracle就发布了五个针对Tuxedo的补丁，修补了5个极高危的漏洞，攻击者可以利用这些漏洞从应用层面获得数据库的完全访问权限，而无需有效的用户名和密码即可获得数据库中的关键数据。内网+多层边界防护是一个丰满的理想，但现实却是骨感的。因为攻击者有可能绕过网络和主机层的“马奇诺防线”，直接从Web应用层打进来。单一边界防护难以保证所谓的内网安全，堆砌式“纵深防御”难以实现“安全网神话”。

多组件系统实现“模块纵深”防御覆盖时，必须实现可信可靠、环环相扣的组件间安全交互机制，才能确保实现的是纵深防御而不是多层堆叠。结合业务流程设置多道防线，有助于阻断攻击获利环节。密文信息的解密环节可重点防护，信息系统在加密等防御保护措施基础上，对解密操作等行为的重点监控，可能给攻击获利环节造成难度，甚至形成威慑效果。

企业传统的城防式安全防护不等于防御纵深，多层堆叠容易沦为马奇诺防线，环环相扣的多层面递进式纵深是最佳防御路径。

（2） 从多个维度分别构建数据纵深防御

① 从安全能力构建数据防御纵深

“IPDRRC”体现了数据保护的时间顺序，基于时间维度，可以有机结合多种安全机制。识别是一切数据保护的前提，在数据识别与分类分级、以及身份识别的前提下，针对数据安全威胁的事前防护、事中检测和响应、事后恢复和追溯反制等多种安全机制环环相扣，协同联动，可以有效构建出面向失效的纵深防御机制。

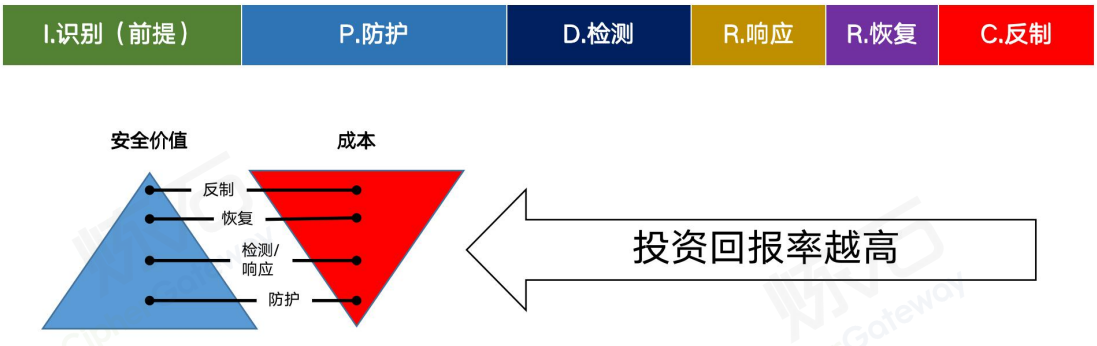

图 5 IPDRRC 投资回报率分布图

当然，从当前企业的数据安全建设重点看，越靠近“事前防护”，投资回报率越高，如果仅依靠检测/响应、恢复以及反制等环节，损失已经发生，企业会付出更高成本。因此，数据安全建设之初，应当优先建设事前防护能力，需要综合应用多种安全技术，尤其是采用密码技术开展数据安全保护，比如加密、脱敏等。

② 从数据形态构建数据防御纵深

数据大致可以分成传输态、存储态和使用态，而身份鉴别及信任体系则是对数据访问的补充或者前提，基于“数据三态”可延伸出数据全生命周期。围绕数据形态，可以构建多种安全机制有机结合的防御纵深。我们梳理出 20 种密码应用模式，采用 IPDRRC 中数据防护段的密码技术，进入了数据形态维度的纵深防御构建。

	身份鉴别及信任体系	数据传输(通信安全)	数据存储(数据资产安全)	数据使用(数据共享与安全兼得)
应用层	① 预共享密钥的身份鉴别 ② 基于私钥签名的身份鉴别 - 单方签名 - 协同签名 -阈值签名	⑤ 离线通信消息加密 - PGP邮件加密 - S/MINE邮件加密 - Signal/OTR聊天加密 ⑥ 代理重加密受控分发消息	⑨ 应用内数据加密 - 应用内加密（集成密码SDK） - CASB代理网关 - 应用内加密（AOE面向切面加密）	⑫ 基于差分隐私的数据匿名化 ⑬ 不可信环境中的数据运算 - FHE全同态加密 - MPC多方安全计算 - ZKP零知识证明、区块链隐私保护 ⑭ 可验证结果的计算外包 ⑮ 基于属性加密的访问控制 ⑯ 锚点解密的防绕过数据安全 - TDF可控分享秘密信息
终端与基础设施层		⑦ 在线通信消息加密 - 基于SSL/TLS的HTTPS - VPN虚拟专用网络 - 链路密码机/网络密码机 ⑧ 可感知窃听的专线通信 - BB84量子密钥分发	⑩ 数据库存储加密 - UDF用户自定义函数加密 - 数据库外挂加密 - TDE透明数据加密 - 数据库加密网关 ⑪ 文件存储加密 - TFE透明文件加密 - FDE全磁盘加密 - DLP终端加密	⑰ 可追溯的数字水印
基础密码产品	③ PKI信任体系 - CA证书认证系统 - 安全认证网关 ④ IBC信任体系			⑱ 基于密码校验的防篡改 - 电子签章 ⑲ 基于私钥签名的责任认定 - 签名验签服务器 ⑳ 封装业务逻辑的可信运算环境 - 金融数据密码机

图 6 二十种密码应用模式一览

在信息系统中，数据在传输、存储、使用等不同形态之间的转化，每时每刻都在发生，在这种转化过程中，可以利用多种安全技术构建协同联动的纵深防御机制。

在传统网络安全防护中，边界是非常重要的概念，边界上可以构建防火墙或IDS等规则。但数据防护过程中，数据没有边界，如果应用密码技术，则可以起到一种虚拟边界的作用，从而在虚拟边界基础上对数据实施保护，形成有效保护作用。在数据存储和使用态的切换中，如果不经过数据加密，只进行访问控制和身份认证，当明文数据在数据库或归档备份时，数据访问容易被绕过。但当我们在数据流转的关键节点上，对数据进行加解密，并结合用户的身份信息和上下文环境做访问控制，可以构建防绕过的访问控制、高置信度的审计，进而在数据存储、使用形态上形成防护纵深，构建出密码安全一体化的数据防护体系。

③ 从技术栈构建数据防御纵深

信息系统的技术栈体现了空间维度，这也可以作为数据保护的纵深。沿着数据流转路径，在典型 B/S 三层信息系统架构（终端侧、应用侧、基础设施侧）的多个数据处理流转点，综合业内数据加密技术现状，总结出适用技术栈不同层次的数据保护技术。我们继续前文所述的 IPDRRC 中数据防护段的密码技术，保护数据存储态，再结合典型信息系统的技术栈分层，可以从技术栈维度构建数据防御纵深。

安全增强点	终端侧	应用层			基础设施层					
	DLP 终端加密	CASB代理网关	应用内加密 (集成密码SDK)	应用内加密 (AOE面向切面加密)	数据库 加密网关	UDF用户 自定义 函数加密	数据库 外挂加密	TDE 透明数据加密	TFE透明 文件加密	FDE 全磁盘加密
实施特点	进程级管控，适用于企业终端数据的安全管理 **优势：**文件外发强管控 **挑战：**终端适配困难、运维成本高	1、通过适配应用层协议和上下文，为已有应用系统增强防护 2、复用CASB平台，降低实施工作量，解决云场景下的信任问题 **优势：**与业务结合的数据安全保护 **挑战：**实施成本较高	1、通过开发改造的方式，与封装了加密业务逻辑的密码SDK集成，调用其加解密接口，使目标应用系统具备数据加密防护能力 **优势：**适用范围广、灵活性高 **挑战：**需要对应用系统开发改造，对应用开发人员要求高	1、对流经切面的数据实施加密脱敏、日志留存及审计等 2、集成应用IAM的终端用户身份信息 3、支持结构化和非结构化数据 **优势：**数据加密与业务逻辑解耦，不影响业务运营，基于细粒度权限控制的数据安全防护 **挑战：**应用程序编程语言和框架需要做适配	1、为数据库提供“入库加密、出库解密”的防护，建立数据库用户的访问控制 **优势：**应用系统与加解密功能分离 **挑战：**只适合开源数据库、高性能和高可用实现难度大	1、改造数据库存储过程，手工编程实现数据加密 **优势：**扩展能力强 **挑战：**通用性低	1、给表增加“触发器+视图”改造，实现入库触发加密、出库视图解密 **优势：**独立权控体系 **挑战：**仅支持Oracle等少量数据库类型、数据库性能损耗较高、可扩展性差	1、国密替换数据库内置算法，支持MySQL/PostgreSQL等，支持国密合规的KMS密管集成 **优势：**独立权控体系、性能损耗较低 **挑战：**防护颗粒度较粗、数据库类型实用性有限制	1、主要执行策略包括文件加密 2、支持Windows/Linux/XC操作系统等 **优势：**可对应用进程接权 **挑战：**管理员风险、高性能实现难度大	1、原理：通过动态加解密技术，对磁盘或分区动态加解密 **优势：**性能优势突出、部署简单 **挑战：**数据防护颗粒度粗

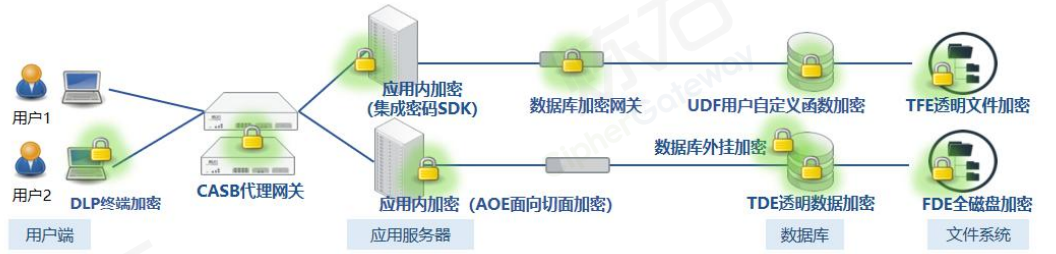

图 7 覆盖不同技术栈的数据存储加密技术

上图列举了 10 种数据存储加密技术，在应用场景以及优势挑战方面各有侧重：DLP 终端加密技术侧重于企业 PC 端的数据安全防护；CASB 代理网关、应用内加密（集成密码 SDK）、应用内加密（AOE 面向切面加密）侧重于企业应用服务器端的数据安全防护；数据库加密网关、数据库外挂加密、TDE 透明数据加密、UDF 用户自定义函数加密则侧重于数据库端的数据安全防护；TFE 透明文件加密、FDE 全磁盘加密则侧重于文件系统数据安全防护。其中，覆盖全量数据的 FDE 技

术可作为基础设施层安全标配，进一步的，针对特别重要的数据再叠加 AOE 等技术实施细粒度加密保护，两者的结合可以面向技术栈构建出数据防护纵深。

综上所述，从安全能力、数据形态、技术栈等多个不同维度上，有机结合多种安全技术构建纵深防御机制，形成兼顾实战和合规、协同联动体系化的数据安全新战法。

进一步的，针对数据本身进行安全技术的“排兵布阵”，可利用先发优势，基于面向失效的设计，布置层层防线，综合利用多样化的手段，构造层层递进式的纵深防御战线，并在一定程度上实现安全与业务的动态平衡。这对于企业数据安全建设来说，必将婴城固守、金城汤池、易守难攻。

四、数据安全框架重点技术详解

4.1 I:识别

在识别战术领域，主要聚焦在数据资产发现和处理，本报告重点对数据资源发现，数据资产识别，数据资产处理（分析），数据分类分级，数据资产打标作出描述。

4.1.1 技术：数据资源发现

■ 基本概念

数据源发现是指对不同类型的数据资源发现的技术，是[战术：识别]的首要工作。数据资源发现非正式定义指：或通过网络流量分析并还原应用协议（被动的），或通过在业务应用嵌入监测锚点（主动的），或利用网络爬虫和扫描引擎探测并请求应用程序接口数据（主动的），以识别网络协议、应用接口、网页、文本、图片、视频、脚本等数据源[3]。

■ 主要实现

数据源发现系列技术主要包括网络流量分析、应用接口探测和业务锚点监测等。

4.1.1.1 扩展技术：网络流量分析

■ 基本概念

[3] 狭义数据源(DataSource)一般指：SUN 制定的用于获取数据库连接的规范接口。本处数据源特指组织的数据资源。

网络流量分析技术是针对网络链路和设备，利用传感器、探针、抓包工具等采集、存储和分析数据，提取协议字段或网络报文内容。

■ 主要实现

网络流量分析技术主要实现方式是利用解码器对二进制网络流量数据和数据包进行还原，解析网络协议，结合上下文特征，分析数据内容。

4.1.1.2 扩展技术：应用接口探测

■ 基本概念

应用接口探测是通过对应用程序接口、应用服务端口或应用数据同步，进行主动扫描，并根据预置权限[4]进行数据资源探测的技术。

■ 主要实现

应用接口探测技术通过端口扫描、网络爬虫、数据同步或消息队列等，探测域名、网页、IP 段、端口、网络协议、应用程序，进一步根据预置协议发现数据资源。其中，端口扫描、网络爬虫、数据同步定义如下：

 # 端口扫描

通过逐个对一段端口或指定端口进行扫描，主机向远端服务器某接口发生连接请求，并记录远端服务器应答，从而得知目标服务器的服务内容，搜集更多有价值信息。

 # 网络爬虫

[4] 应用服务的低权限账号、口令或接口请求参数。

也称网络机器人，是指按照一定的规则，自动地抓取万维网信息的程序或者脚本。

 # 数据同步

利用后台程序编码进行数据同步，或利用发布/订阅、SQL JOB、消息队列等进行数据同步。

4.1.1.3 扩展技术：业务锚点监测

■ 基本概念

业务锚点监测是指分析业务应用中数据流转，在业务功能或网络环节中，实施埋点或者部署切面，实现对业务数据监测的技术。

■ 主要实现

业务锚点监测技术的主要实现方式为利用在客户端埋点、服务端埋点；利用配置或代码记录所有业务操作和内容。

4.1.2 技术：数据资产识别

数据资源的资产属性，且一般归类为无形资产[21]。由于数据资产[5]属性，在开展数据安全工作时，首先对数据资产识别是常见技术手段之一。

数据资产识别非正式定义为：结合组织的行业属性，利用文本识别（音频转义）、图像识别（视频分帧）等技术，通过关键字匹配，正则表达式匹配以及其它自动化识别技术，对数据资源信息、构成等进行资产属性挖掘。

[5] 根据 DMBOK1.0, 2014，数据资产(Data Asset)是指由企业拥有或企业控制的，能够为企业带来未来经济利益的，以物理或电子的方式记录的数据资源，如文件资料、电子数据等。在企业中，并非所有的数据都构成数据资产，数据资产是能够为企业产生价值的数据资源。

数据资产识别一般为数据资源发现后置动作，一般为数据资产处理、数据分类分级前置动作[6]。

■ 基本概念

数据资产，是指拥有数据权属（勘探权、使用权、所有权）、有价值、可计量、可读取的网络空间中的数据集。

■ 主要实现

数据资产识别的主要实现方式为利用自动化技术手段对企业数据进行筛选与分析,找出符合数据资产定义的数据集。数字资产的识别技术主要包含关键字、正则表达式、基于文件属性识别、精准数据比对、指纹识别技术和支持向量网络等。

4.1.2.1 扩展技术：关键词提取

随着NLP、OCR、ASR等技术不断成熟，针对自然语言样本数据进行关键词提取得到进一步推广。关键词提取在智能文档审阅、机器人流程自动化等领域已经有了较成功应用，特别地，把结合AI算法、机器学习的关键词提取技术在数据资产识别场景下是较为成熟的应用技术。

■ 基本概念

关键词提取指运用人工确认、自动化算法等，自动抽取反映文本主题的词或者短语的过程、技术和方法。在数据安全领域，关键词可以用来识别和标记有价值的数据资产。

[6] 在非特定场景下，数据资源发现、数据资产识别、数据资产处理（分析）会由一体化产品或方案实现。

■ 主要实现

关键词提取一般会集成于推荐系统或搜索系统，提取方法分为有监督[7]、半监督和无监督。其中，无监督关键词抽取算法可以分为三大类，基于统计特征的关键词抽取、基于词图模型的关键词抽取和基于主题模型的关键词抽取。

 # 基于统计特征的关键词提取算法

利用文档中词语的统计信息抽取文档的关键词。通常将文本经过预处理得到候选词语的集合，然后采用特征值量化的方式从候选集合中得到关键词。基于统计特征的关键词抽取方法的关键是采用什么样的特征值量化指标的方式，常用的有三类：

1) 基于词权重的特征量化

2) 基于词的文档位置的特征量化

3) 基于词的关联信息的特征量化

 # 基于词图模型的关键词抽取算法

构建文档的语言网络图，对语言进行网络图分析，图上确认的具有重要作用的词或者短语即为关键词。根据词的链接方式不同，语言网络的主要形式分为四种：

1) 共现网络图、

2) 语法网络图、

3) 语义网络图

[7] 有监督的文本关键词提取算法需要高昂的人工成本，本文重点关注无监督关键词提取算法。

4) 其他网络图

 # 基于主题模型的关键词抽取

利用的是主题模型中关于主题的分布的性质进行关键词提取。算法的关键在于主题模型的构建。

4.1.2.2 扩展技术：正则表达式

在可控的数据资源范围内，识别未知数据资产或者检测发现流量中动态数据，利用正则表达式是较高效较精准的识别方法。

■ 基本概念

正则表达式(regular expression)指利用字符串匹配的模式（pattern），来检查一个字符串是否含有某种子串、将匹配的子串替换或者从某个串中取出符合某个条件的子串等。在数据安全领域，可以通过正则表达式搜索拥有特定属性的数据资产。

构造正则表达式的方法和创建数学表达式的方法一样。也就是用多种元字符与运算符可以将小的表达式结合在一起来创建更大的表达式。正则表达式的组件可以是单个的字符、字符集合、字符范围、字符间的选择或者所有这些组件的任意组合。

■ 主要实现

正则表达式是由普通字符（例如字符 a 到 z）以及特殊字符（称为"元字符"）组成的文字模式。模式描述在搜索文本时要匹配的一个或多个字符串。正则表达式作为一个模板，将某个字符模式与所搜索的字符串进行匹配。

正则表达式的主要实现方式为采用多种元字符与运算符，将小的表达式结合，创建更大的表达式。正则表达式的组件可以是单个字符、字符集合、字符范围、字符间的选择，也可以是这些组件的任意组合。

通常，正则表达式的语法为：

#普通字符

包括没有显示指定为元字符的所有可打印和不可打印字符。这包括所有大写和小写字母、所有数字、所有标点符号和一些其他符号。

#非打印字符

非打印字符也可以是正则表达式的组成部分，如\cx\f\n 等。

#特殊字符

一些有特殊含义的字符，如“runoo*b”中的“*”。其中，许多元字符要求在试图匹配它们时特别对待。

#限定符

用来指定正则表达式的一个给定组件必须要出现多少次才能满足匹配。有 * 或 + 或 ? 或 {n} 或 {n,} 或 {n,m} 共 6 种。

#定位符

可以将正则表达式固定到行首或行尾，还可以创建出现在一个单词内、在一个单词的开头或者一个单词的结尾的正则表达式。

#选择

用圆括号 () 将所有选择项括起来，相邻的选择项之间用 | 分隔。() 表示捕获分组，() 会把每个分组里的匹配的值保存起来，多个匹配值可以通过数字 n 来查看(n 是一个数字，表示第 n 个捕获组的内容)。

#反向引用

对一个正则表达式模式或部分模式两边添加圆括号将导致相关匹配存储到一个临时缓冲区中,所捕获的每个子匹配都按照在正则表达式模式中从左到右出现的顺序存储。缓冲区编号从 1 开始，最多可存储 99 个捕获的子表达式。每个缓冲区都可以使用\n 访问，其中 n 为一个标识特定缓冲区的一位或两位十进制数。[8]

常见车牌正则表达式：

/^([京津沪渝冀豫云辽黑湘皖鲁新苏浙赣鄂桂甘晋蒙陕吉闽贵粤青藏川宁琼使领

A-Z]{1}[a-zA-Z](([DF]((?![IO])[a-zA-Z0-9](?![IO]))[0-9]{4})|([0-9]{5}[DF]))|[京津沪渝冀豫云辽黑湘皖鲁新苏浙赣鄂桂甘晋蒙陕吉闽贵粤青藏川宁琼使领

A-Z]{1}[A-Z]{1}[A-Z0-9]{4}[A-Z0-9 挂学警港澳]{1})$/

常用居民身份证(18 位)正则表达式：

/^[1-9]\d{5}(18|19|([23]\d))\d{2}((0[1-9])|(10|11|12))(([0-2][1-9])|10|20|30|31)\d{3}[0-9Xx]$ /

4.1.2.3 扩展技术：基于文件属性识别

据 IDC 研究表明，到 2025 年，全球数据量将会从 2016 年的 16 ZB 上升至 163ZB。著名研究机构 Garter 也表示，全球信息量正在以 59%以上的年增长率快速增长，其中 80%都是以文件形式存在的非结构化和半结构化数据；在半结构化中，日志文件、机器数据等又占比 90%。

[8] 正则表达式 - 语法，https://www.runoob.com/regexp/regexp-syntax.html

利用日志文件、机器数据的文件属性进行粗较度数据资产识别是数据资产识别重要手段之一。

■ 基本概念

文件属性[9]识别指基于文件属性对文件进行识别和分类。文件属性识别在数据安全领域，可以用来对数据资产进行识别和分类，从而更高效处理和利用数据资产。

■ 主要实现

文件属性识别的主要实现方式包括聚类识别、文件相似度、文件精确指纹识别、文件 DNA 识别、支持多属性条件过滤等技术。

 # 聚类识别

根据文件业务内容，基于大量行业文件进行机器学习，智能识别分类文件，如财务文件聚类、金融行业文件聚类等。

 # 文件相似度

根据文件内容相似度比例，找到与此文件相关联的文件。

 # 文件精确指纹识别

根据提取计算的文件指纹，准确识别。

 # 文件 DNA 识别

根据文件的内容特征，发现由此文件编辑、修改后保存的不同版本的文件。

[9] 文件属性指为了区分不同类型的文件，而定义的文件的某种独特性质。常见的文件属性分为系统属性、隐藏属性、只读属性和归档属性。

 # 支持多属性条件过滤

支持匹配次数、文件大小、优先级、文件类型等过滤。

4.1.2.4 扩展技术：精确数据比对

在数据资产识别场景中,往往需要精准地发现某一类数据资产,比如通过“名字”、“身份证号”、“手机号码”、“银行帐号”来识别高可置信的个人敏感信息。

■ 基本概念

精确数据比对（EDM）指预先对数据库存储数据进行扫描学习，梳理数据结构，了解资产分布与范围，标定敏感等级，形成关键词信息索引的技术，EDM 通常用于保护结构化格式的数据。

■ 主要实现

精确数据比对的主要实现方式为根据特定数据列中的任何数据栏组合进行检测，即在特定记录中检测 M 个字段中的 N 个字段，能在“值组”或指定的数据类型集上触发。

4.1.2.5 扩展技术：指纹文档比对

在非结构化数据识别过程中，我们需要对已创建的文档进行不同版本，不同格式进行差异化管理。在类似场景中，指纹文档比对 (IDM) 可确保准确检测以文档形式存储的非结构化数据。[22]

■ 基本概念

指纹文档比对（IDM）指通过创建文档指纹特性，以检测原始文档的已检测部分、草稿或不同版本的受保护文档的技术，主要用于检测以文档形式存储的非结构化数据。[23]

■ 主要实现

指纹文档比对要进行敏感文件的学习和训练，拿到敏感内容的文档时，采用语义分析的技术进行分词、语义分析，提取需要学习和训练的敏感信息文档的指纹模型，利用同样的方法对被测的文档或内容进行指纹抓取，将得到的指纹与训练的指纹进行比对，根据预设的相似度去确认被检测文档是否为敏感信息文档。

4.1.2.6 扩展技术：向量分类比对

在开展数据资产识别场景中，部分数据很难用关键词、正则表达式以及精确数据比对等方法来定义或描述。向量分类比对（SVM）方法可以预先定义文档内容类别，根据特征进行SVM比对，并提取文档的权限和策略。

■ 基本概念

向量分类比对（SVM）指依靠建立在统计学习理论的VC维理论和结构风险最小化原理基础上,利用有限的样本所提供的信息对模型的复杂性和学习能力两者进行了寻求最佳的折中，以获得最好的泛化能力的技术。原理总结是，SVM是将待检测文件向量化，并归属到某一类训练集所建立的向量空间。SVM通常也适用于保护非结构化的数据，尤其适用于财务报告和源代码等数据形式。

■ 主要实现

向量分类比对的主要实现方式为支持向量机。支持向量机是基于结构风险最小化原理(SRM)，为了控制泛化能力，需要控制两个因素，即经验风险和置信范围值。传统的神经网络是基于经验风险最小化原则，以训练误差最小化为优化目标，而支持向量机以训练误差作为优化问题的约束条件，以置信范围最小化为优化目标。[24]

4.1.3 技术：数据资产处理（分析）

当前，常规的、可控的、静态的数据分类分级已有较好的技术支撑，但针对多格式的、自动采集、动态的数据安全分类分级特别要求在数据资产识别后，需要优先进行数据资产处理。

■ 基本概念

数据资产处理（分析）指在数据清洗的基础上，针对已采集和识别的重要数据资产和个人信息进行合规和安全处理。

■ 主要实现

通常，数据资产处理（分析）要首先对数据内容进行识别，然后再进行安全性分析、合规性分析、重要性（敏感性）分析等。

4.1.3.1 扩展技术：数据内容识别

数据内容识别与数据资产识别技术实现类似，但侧重点不一。数据资产识别重点找出数据资源特别，结合资产属性，自动化梳理和识别出资产保护目录。数据内容识别要求对整个数据进行全文识别，旨在发现。

■ 基本概念

数据内容识别，主要指针对结构化以及非结构化的数据内容进行识别，识别范围覆盖网页、邮件传输、终端刻录、拷贝传输等。数据内容识别能够为了对敏感数据进行控制和管理。

■ 主要实现

数据内容识别主要实现方式包括文字识别、图片识别、语音识别等技术。

 # 文字识别

基于行业前沿的深度学习技术，提供通用印刷体识别、通用印刷体识别（高精度版）、通用手写体识别、英文识别等多种服务，支持将图片上的文字内容，智能识别为可编辑的文本，可应用于随手拍扫描、纸质文档电子化、电商广告审核等多种场景，大幅提升信息处理效率。

 # 图片识别[10]

对图像进行对象识别，以识别各种不同模式的目标和对象的技术。图像识别是立体视觉、运动分析、数据融合等实用技术的基础，在导航、地图与地形配准、自然资源分析、天气预报、环境监测、生理病变研究等许多领域重要的应用价值。

 # 语音识别，又称自动语音识别 Automatic Speech Recognition，(ASR)，其目标是将人类的语音中的词汇内容转换为计算机可读的输入，例如按键、二进制编码或者字符序列。与说话人识别及说话人确认不同，后者尝试识别或确认发出语音的说话人而非其中所包含的词汇内容。

[10] 有效的视频内容识别多为抽帧分析，故本文不分析视频内容识别。

4.1.3.2 扩展技术：合规性分析

在数据采集识别后，要首先进行合规性分析，比如政策合规性、法律合规性、行业监管合规性等。

■ 基本概念

合规性分析在数据内容识别后，利用人工专家或自动化研判模型，通过合规性评估，帮助企业或组织提升系统的数据内容合规安全保障能力，从而实现持续安全运营，能够更好符合数据安全相关的法律法规、标准及规范，保证业务数据的合规、合法。

■ 主要实现

目前，合规性分析主要分为违法信息识别、未成年人信息识别、侵权识别、个人敏感信息识别、商业秘密识别、重要数据识别等。主要通过在数据处理过程的采集、传输、存储环节，部署软硬模块实现合规管理。

 # 采集环节合规处理

在数据采集时，在采集终端或上传接口，增加软数据词法、特征分析模块，主动告警、删除违规、违法数据。

 # 传输环节合规处理

在数据传输时，部署数据合规性处理网关，发现和拦截违规、违法数据。

 # 存储环节合规处理

在数据被集中清洗或统一存储时，或在数据预处理，或在数据落地存储，发现和拦截违规、违法数据。

在部分数据安全工作场景中，需要对特定数据进行合规性分析，比如在做行业数据安全监管时，需要对数据加密后格式，加密算法进行识别与合规性处理，通过会应用行业内专用工具进行数据合规处理。比如，密评工具箱。

 # 密评工具箱

将密评确定性的检测内容进行工具化实现，辅助评测机构测评以及企业自测。密评工具箱支持以旁路部署的方式接入目标环境中，通过采集样本数据、密文分析判定、密码算法还原等功能和方法，快速判定目标系统是否用了密码、用的密码是否是国密算法、用的国密是否安全有效，为密评工作提供有力支撑。[11]

4.1.3.3 扩展技术：安全性分析

在进行数据的合规性分析[12]后，要考虑数据安全性分析。对于采集的或录入系统的结构化数据可能被引入攻击指令、非法数据操作，对于采集的或录入系统的结构化数据可能被引入恶意程序、攻击脚本以及其它非法代码等。

■ 基本概念

安全性分析指利用部分数据资产识别扩展技术以及网络安全终端防护、服务器防护技术，通过合安全性评估，帮助企业或组织提升系统的数据安全保障能力，从而实现持续安全运营，能够更直接降低非法数据集引入恶意攻击。

■ 主要实现

[11] 密评工具箱，http://www.ciphergateway.com/product/38916.html
[12] 二者可以调整先后顺序

除了，恶意代码检测、恶意 APP 分析、僵木蠕系统等应用，数据沙盒技术（Data Sandbox）可提供较高可靠的安全性分析。

 # 数据沙盒技术[13]

多为以虚拟方式模拟一个终端或一个运行环境，检测未知代码在该虚拟环境中的运行状况，并根据运行状况来判断其是否是怀有恶意。特别地，数据沙盒技术可以应用于大数据领域，不对原始数据进行拷贝和分析，搜索原始的结构化或非架构化的数据，形成新的数据信息仓库。根据事先定义的分析引擎去对提取的信息进行关联分析。[25]

4.1.3.4 扩展技术：重要性（敏感性）分析

重要性（敏感性）分析是合规性分析的一个重要延伸。合规性分析更多是多违规、违法数据的处理（即不在组织运营或权责范围内的数据进行处理）。重要性（敏感性）分析聚焦在组织权责范围内运营的数据进行数据重要程度和个人信息的敏感程度进行分析。

■ 基本概念

重要性（敏感性）分析指通过设置各种环境敏感数据类别和数据安全性等级，设置敏感数据检索系统，不间断对各种环境数据进行敏感性检测，发现并标识各类敏感数据，并进行相应保护等级的标准。

■ 主要实现

[13] 数据沙盒先可以结合合规性规则，实现对数据安全法、网络安全审查管理办法、GDPR、PII 等中国、欧美合规要求，帮助企业更好地确保企业拥有敏感数据的私密性。

针对结构化数据的重要性（敏感性）分析是当前数据安全重点工作之一。结构化数据的重要性（敏感性）分析主要实现方式为通过定期全库扫描，识别敏感字段（周期触发）；新增或修改表和字段，增量扫描识别出敏感字段；监听数据库对表或字段，指定表或字段进行敏感识别扫描，结合数据库代理服务；手动触发扫描。具体方法如下：

#　基于元数据的敏感数据识别（敏感词库+关键词匹配）

定义敏感数据的关键词匹配式，通过精确或模糊匹配表字段名称、注释等信息，利用元数据信息对数据库表、文件进行逐个字段匹配，当发现字段满足关键词匹配式时，判断为敏感数据并自动定级。这种匹配方式成本低、见效快，可识别全网 50%以上的客户敏感数据。

#　基于数据内容的敏感数据识别（正则表达式）

有些临时表或历史上开发的未按照规范建立的敏感表，根据元数据无法判断是否为敏感数据，这种情况更多是靠分析数据内容来判断。自动化工具通过扫描获取这些表，将系统中大量数值型、英文型的敏感信息（如手机号、身份证号、邮箱等）通过预先定义正则表达式的方式进行匹配，做出敏感数据及其级别的判定。

#　基于自然语言处理技术的中文模糊识别（敏感词库+分词+相似度计算）

前面两种方式可以发现系统中大部分的客户敏感数据，但系统中还保存了部分中文信息，无法通过上述两种方式很好地发现。因此，引入 NLP 自然语言处理技术加中文近似词比对的方式进行识别。首先，根据数据内容整理输出一份常用敏感词，该敏感词列表需具备一定的学习能力，可以动态添加敏感

词；其次，通过NLP对中文内容进行分词，通过中文近似词比对算法计算分词内容和敏感词的相似度，若相似度超过某个阈值，则认为内容符合敏感词所属的分类分级。[31]

4.1.4 技术：数据分类分级

■ 基本概念

数据分类分级需要分两个步骤来开展。数据分类指根据组织数据的属性或特征，将其按照一定的原则和方法进行区分和分类，并建立起一定的分类体系和排列顺序，以便更好地管理和使用组织数据的过程。数据分级指按照一定的分级原则对分类后的数据进行定级，从而为数据的开放和共享安全策略提供支撑。

■ 主要实现

数据分类分级主要实现方式为依据标签库、关键词、正则表达式、自然语言处理、数据挖掘、机器学习等内容识别技术，进行数据分类，根据数据分类的结果，依据标签进行敏感数据的划分，最终实现数据分级的效果。数据分类分级技术按元数据类型可分为：

 # 内容感知分类技术

对非结构化数据内容的自动分析来确定分类，涉及正则表达式、完全匹配、部分或完整指纹识别、机器学习等。

 # 情境感知分类技术

基于数据特定属性类型，利用广泛上下文属性，适用于静态数据（如基于存储路径或其他文件元数据）、使用中的数据（如由 CAD 应用程序创建的数据）和传输中的数据（基于 IP）。

按实际应用场景分类技术：

 # 根据分类分级规则

建立标签库，利用机器学习算法经过训练形成分类器，利用分类器将生成的分类器应用在有待分类的文档集合中，获取文档的分类结果，并可进行自动化打标。[27]

4.1.4.1 扩展技术：自动化工具

■ 基本概念

自动化工具，是指数据分类分级场景下的自动化处理的工具。自动化工具主要指基于数据分类分级方面的基本准则和技术，进行自动化的识别、分类以及定级的过程。自动化工具适合大量数据的分类分级处理。

■ 主要实现

 # 自动化数据分类分级平台

通过自动化技术，将分类分级的专家经验和方法固化为规则模型和识别引擎，有效避免采用全人工进行数据分类分级时存在的因人员经验背景知识不足导致的不确定性问题，降低人力成本。同时，在具体实施过程中根据不同场景，可与数据资产管理系统、传统数据库、大数据库等进行对接，还可根

据不同行业选择不同的识别引擎，通过识别关键要素，结合分类分级的规则进行自动化分类分级。

 # 自动化数据分类分级打标

通过对数据打标签的方式降低数据安全管理的门槛，帮助企业进行数据的分类管理，分级防护。目前，业内的专用工具可基于关联补齐后的数据，结合数据分类分级结果，在原数据基础上进行标记。[28][29][30]

4.1.4.2 扩展技术：人工辅助

■ 基本概念

人工辅助，指数据分类分级场景下的人工辅助系统。人工辅助系统主要指人工建立的、预定用来求解数据分类分级问题的系统，能够为决策人提供帮助和支持。该系统可以对信息进行检索、处理和存储，能在分类分级的每个阶段提供精确且高效的服务。

■ 主要实现

人工辅助的主要实现方式为通过人工检查的方式，定期回顾数据打标签的正确性、敏感数据的存储使用状态等。

4.1.5 技术：数据资产打标

■ 基本概念

数据资产打标指在生产过程中，依据国家相关规定或企业自身管理需求，在产品上通过各种技术进行文字、图片等标识，产品并不局限于实体。

■ 主要实现

数据资产打标的主要实现方式包括：基于关键字的敏感数据打标：通过字段名称，注释信息；基于正则的敏感数据打标：通过样本数据；基于机器学习的敏感数据打标：整个表中所有字段名，样本数据，与其他表的相似度进行训练；对账号字段打标等。

4.1.5.1 扩展技术：标记字段法

■ 基本概念

标记字段法，是指把标记“打”在某一个公共访问的字段上面的技术手段。这个字段往往代表了数据的一种属性,从而能够作为区分数据资产方式的一个重要依据。

■ 主要实现

标记字段法的主要实现方式为自动获取企业所有数据库、所有表、所有字段，根据字段的值，利用正则表达式等方式判断此字段是否属于用户敏感信息，如姓名、手机、地址、身份证等。最终形成数据的风险地图，库、表、字段、敏感类型和等级，可以为统一加解密、统一日志等提供服务。[26]

4.1.5.2 扩展技术：元数据映射表法

■ 基本概念

元数据映射表法，是指利用元数据建立映射表，然后便于寻找相关数据的一种技术手段。元数据是指描述数据的数据，主要描述数据的属性信息，用来支持如指示存储位置、历史数据、资源查找、文件记录等功能。映射表则主要用来存放键值对，如果提供相应的键，就能查到相应的值。

■ 主要实现

元数据映射表法主要实现方式为编译前根据元数据生成映射代码、在运行期根据元数据通过反射实现映射。[32][33]

4.1.5.3 扩展技术：数字水印法

■ 基本概念

数字水印法，是指通过数字水印的方式，为数据资产打标。数据水印是基于信息安全、信息隐藏、数据加密等技术，在数据文件页面中增加不可篡改的明水印或肉眼无法识别的隐水印，实现对数据文件原始确权唯一性的确认。

■ 主要实现

数字水印的主要实现方式灰度值加密、位置加密、双因子加密等方法。[34][35][36]

 # 灰度值加密

图像的灰度值直方图本质上是一种表示数字图像各级灰度值及其出现频数关系的函数，描述的是图像中具有的该灰度值的像素的个数。像素灰度值加密是利用混沌映射产生的灰度值扰乱向量(矩阵)，对原始图像像素值进行扰乱，达到隐藏图像信息的目的。灰度值加密使用两个矩阵进行异或后得到。

 # 位置加密

利用混沌行为的不可重复、不可预测和初始条件极端敏感的特性，经过对混沌序列进行处理，产生混沌位置扰乱向量或者说混沌位置置乱矩阵，来改变像素在原始图像矩阵中的位置，达到图像不可读，掩盖图像信息的目的。

 # 双因子加密

为了增强安全性，采用位置加密和灰度值加密相结合(双因子加密) 的方法对水印图像进行加密。这种加密方法可降低在水印图像遭受提取时水印被破译的概率，确保水印的安全保密性。

4.2 P:防护

在防护战术领域，重点考虑识别战术后，围绕数据资产展开的主动、被动安全保护技术手段，故对于未直接作用于数据本身的保护技术手段暂未收录[14]。

4.2.1 技术：数据加密技术

■ 基本概念

数据加密指通过加密算法和加密密钥将明文转变为密文，而解密则是通过解密算法和解密密钥将密文恢复为明文。

■ 主要实现

利用加密算法、加密协议以及加密产品，对存储态数据、传输态数据、使用态数据实现密文到明文相互转化。

4.2.1.1 扩展技术：存储加密

■ **基本概念**

在存储介质主程序启动前加载加密程序，实现在数据写入存储介质前将数据进行加密，实现数据的存储加密，在存储介质加载数据到内存前进行数据解密，实现数据的解密使用。

[14] 例如，网络欺骗防御技术在网络安全领域具有较高价值，但由于技术非“以数据为中心“，故本文不作收录。

■ 主要实现

利用密码技术将数据转换成密文存储后，可防止存储环节中的泄密。

DLP 终端加密

在受管控的终端上安装代理程序，由代理程序与后台管理平台交互，并结合企业的数据管理要求和分级分类策略，对下载到终端的敏感数据进行加密，从而将加密应用到企业数据的日常流转和存储中。信息被读取到内存中时会进行解密，而未授权复制到管控范围外则是密文形式。

CASB 代理网关

将网关部署在目标应用的客户端和服务端之间，无需改造目标应用，只需通过适配目标应用，对客户端请求进行解析，并分析出其包含的敏感数据，结合用户身份，并根据设置的安全策略对请求进行脱敏等访问控制，可针对结构化数据和非结构化数据同时进行安全管控。

应用内数据加密（集成密码 SDK）

应用内加密（集成密码 SDK）是指应用系统通过开发改造的方式，与封装了加密业务逻辑的密码 SDK 进行集成，并调用其加解密接口，使目标应用系统具备数据加密防护能力。

应用内加密（AOE 面向切面加密）

数据安全插件部署在应用服务中间件，结合旁路部署的数据安全管理平台、密钥管理系统，通过拦截入库 SQL，将数据加密后存入数据库。

数据库加密网关

数据库加密网关是部署在应用服务器和数据库服务器之间的代理网关设备，通过解析数据库协议，对传入数据库的数据进行加密，从而获得保护数据安全的效果。

数据库外挂加密

数据库外挂加密通过针对数据库定制开发外挂进程，使进入数据库的明文先进入到外挂程序中进行加密，形成密文后再插入数据库表中。这种技术使用“触发器”+“多层视图”+“扩展索引”+“外部调用”的方式实现数据加密，可保证应用完全透明。通过扩展的接口和机制，数据库系统用户可以通过外部接口调用的方式实现对数据的加解密处理。视图可实现对表内数据的过滤、投影、聚集、关联和函数运算，在视图内实现对敏感列解密函数的调用，实现数据解密。

TDE 透明数据加密

在数据库内部透明实现数据存储加密、访问解密的技术，Oracle、SQL Server、MySQL 等数据库默认内置此功能。数据在落盘时加密，在数据库内存中是明文，当攻击者“拔盘”窃取数据，由于数据库文件无法获得密钥而只能获取密文，从而起到保护数据库中数据的效果。

UDF 用户自定义函数加密

在数据库支持的形式上，通过定义函数名称及执行过程，实现自定义的处理逻辑。UDF 用户自定义函数加密，是通过 UDF 接口实现数据在数据库内的加解密。

TFE 透明文件加密

在操作系统的文件管理子系统上部署加密插件来实现数据加密，基于用户态与内核态交付，可实现“逐文件逐密钥”加密。

FDE 全磁盘加密

通过动态加解密技术，对磁盘或分区进行动作加解密的技术。FDE 的动态加解密算法位于操作系统底层，其所有磁盘操作均通过 FDE 进行：当系统向磁盘上写入数据时，FDE 首先加密要写入的数据，然后再写入磁盘；反之，当系统读取磁盘数据时候，FDE 会自动将读取到的数据进行揭秘，然后再提交给操作系统。

可互操作存储加密

把加密算法和密钥管理集成于自加密驱动器（SED），简单用户使用移动存储、移动设备时，复杂的密码技术设置与操作。

4.2.1.2 扩展技术：传输加密

■ 基本概念

传输加密技术是对传输中的数据流加密，保证传输通道、传输节点和传输数据的安全，防止通信线路上的窃听、泄漏、篡改和破坏。

■ 主要实现

通常传输加密技术可分为线路加密和端到端加密。其中，线路加密指对保密信息通过各线路采用不同的加密密钥提供安全保护；端到端加密指信息由发送端

自动加密，并且由 TCP/IP 进行数据包封装，然后作为不可识别的数据经互联网传输，在信息到达目的地，将被自动重组、解密，而成为可读的数据。

此外，根据传输加密的数据对象状态不同，又可分为在线通信消息传输加密和离线通信消息传输加密。

 # 离线通信消息传输加密

利用密码学算法和密码协议，构建安全协议或通信框架，在数据在网络传输前把数据源加密为密文，经过网络传输后，再对密文进行解密。常见的离线通信消息传输加密包含：

1) **PGP 邮件加密，**PGP（Pretty Good Privacy）是一种加密系统，主要用于发送加密电子邮件和加密敏感文件。当下 PGP 已成为电子邮件安全事实标准。PGP 加密系统是采用公开密钥加密与传统密钥加密相结合的一种加密技术。它使用一对数学上相关的钥匙，其中一个（公钥）用来加密信息，另一个（私钥）用来解密信息。

2) **S/MINE 邮件加密，**S/MIME 是指 (安全多用途互联网邮件扩展协议)，是采用 PKI 技术的用数字证书给邮件主体签名和加密的国际标准协议，其优势在于不仅仅是邮件加密，而且还能为邮件带上邮件发送者的通过第三方 CA 验证的真实身份信息，以便收件人能确信发件人的真实身份。

3) **Signal/OTR 聊天加密，**Signal，是指一对一的加密协议，该协议采用“Ratchet 棘轮”系统，该系统在每条消息后更改密钥，主要通过为每个用户生成除永久密钥之外的一组临时密钥来实现此目的。在聊天加密场景中，每次发送消息，密钥都会更新。使用该协议，意味着即使用户手

机某一时刻被盗，但之前发送的任何消息都是安全的。OTR 指一款安全的加密协议，它主要提供将即时聊天和通讯内容进行强加密的服务。OTR 作为一种聊天协议，它不会留下任何记录，是一种为即时消息加密的加密协议。

4) **安全即时通信，与 Signal/OTR 聊天加密类似，安全即时通信**考虑即时通信系统安全特性，在即时通信协议的基础上，采用基于 SSL/TLS 的双向认证、传输加密技术、基于 PKI 体系的数据加密技术、文件密级标识技术，实现安全即时通信平台。

 # 在线通信消息传输加密

利用计算机实现，在发送端，通过运行在计算机中的软件对消息进行加密，然后通过装置发功，在加手段收到加密的消息后，传送给计算机，再通过相应的软件进行解密。

 # 可感知窃听的专线通信传输加密技术

量子密钥分发技术是量子通信的实现方式之一，利用量子力学将一个真随机数密码本安全地分配给通信双方，以供后续加解密使用。在量子密钥分发过程中，密钥的生成采用单光子的状态作为信息载体来实现，因为光量子具有不可分割且量子态无法复制的特性，即使窃听者使用先进的窃听方式，光量子在量子信道传输过程中也无法被破译和窃听，从而确保了量子密钥分发的安全性。

 # 代理重加密受控分发消息传输加密技术

代理重加密，是指委托可信第三方或是半诚实代理商将自己公钥加密的密文转化为可用另一方私钥解开的密文从而实现密码共享。在云计算与云存储中，一种场景需求是用户 A 期望通过云存储平台向用户 B 共享秘密数据，而这些数据显然不能被云平台获知。代理重加密可以实现，用户 A 利用自己的公钥对数据进行加密后上传，云端对密文进行计算处理后使得这一密文数据可以令任一指定用户 B 的私钥进行解密。

4.2.1.3 扩展技术：使用加密

■ **基本概念**

通过在数据使用过程中采取加密技术手段,防止数据使用过程中数据本身及数据计算过程机密性、完整性、可用性被破坏。

■ **主要实现**

 # FHE 全同态加密

由全同态加密方案产生的密文，可以对密文进行任意计算，解密结果与对名为进行相应计算的结果相同，实现数据处理权和使用权的分离，防止数据泄漏的同时，充分利用外部算力。

 # MPC 多方安全计算

MPC 安全多方计算,允许多个数据所有者在互不信任的情况下进行协同计算，输出计算结果，并保证任何一方均无法得到除应得的计算结果之外的其他任何信息。MPC 技术可以获取数据使用价值，却不泄露原始数据内容，该技术有输入隐私性、计算正确性及去中心化等特性。

ZKP 零知识证明

零知识证明（ZKP），是一种基于概率的验证方式。验证者基于一定的随机性向证明者提出问题，如果证明者都能给出正确回答，则说明证明者大概率拥有他所声称的“知识”。零知识证明并不是数学意义上的证明，因为它存在小概率的误差，欺骗的证明者有可能通过虚假的陈述骗过验证者。换句话说，零知识证明是概率证明而不是确定性证明，但是也存在技术能将误差降低到可以忽略的值。

可验证计算

可验证计算是指不泄露用户隐私并验证外包服务的计算结果，用户将需要计算的函数和输入数据加密后发给服务提供者，由服务提供者返回计算结果及对结果的证明。用户可验证计算结果的正确性，且验证的计算量远远小于直接计算函数。

可信执行环境

可信执行环境（Trusted Execution Environment，TEE）指在计算平台上由软硬件方法构建的一个安全区域，可保证在安全区域内加载的代码和数据在机密性和完整性方面得到保护，确保一个任务按照预期执行，保证初始状态的机密性、完整性，以及运行时状态的机密性、完整性。

目前成熟的技术主要有：Intel SGX、ARM TrustZone、AMD SEV 和 Intel TXT。

4.2.2 技术：数据脱敏技术

- 基本概念

数据脱敏又称为数据漂白、数据去隐私话或数据变形。是指从原始环境向目标环境进行敏感数据交换的过程中，通过一定方法消除原始环境数据中的敏感信息，并保留目标环境业务所需的数据特征或内容的数据处理过程。既能够保障数据中的敏感数据不被泄露又能保证数据可用性的特性，使得数据脱敏技术成为解决数据安全与数据经济发展的重要工具。[37]

■ 主要实现

数据脱敏主要包括动态脱敏技术、静态脱敏技术、隐私保护技术等。

4.2.2.1 扩展技术：动态脱敏技术

■ 基本概念

对不同身份、不同权限的用户可配置实时数据脱敏规则，对敏感数据进行屏蔽、遮盖、变形处理，结合用户身份和权限将脱敏后结果展示给用户，有效防止敏感数据泄漏。

■ 主要实现

当应用系统请求通过动态数据脱敏时，基于代理技术，实时筛选请求的SQL语句，依据用户角色、权限和其他脱敏规则屏蔽敏感数据，并且能运用横向或纵向的安全等级，同时限制响应一个查询所返回的数据。

4.2.2.2 扩展技术：静态脱敏技术

■ 基本概念

静态脱敏技术，通常用于非生产环境，将敏感数据从生产环境抽取并脱敏后给到非生产环境使用，一般用于对非实时访问的数据进行数据脱敏，数据脱敏前统一设置好脱敏策略，并将脱敏结果导入到新的数据中，包括文件或者数据库中。

■ 主要实现

静态脱敏直接通过屏蔽、变形、替换、随机、格式保留加密（FPE）和强加密算法（如 AES）等多种脱敏算法，针对不同数据类型进行数据掩码扰乱，并可将脱敏后的数据按用户需求，装载至不同环境中。

4.2.2.3 扩展技术：隐私保护技术

■ 基本概念

隐私保护技术作为一种新兴的信息安全技术，其特性是对外公开的、自由访问，其核心是要保护隐私数据与个人之间的对应关系。[38]

■ 主要实现

通过切断攻击者到隐秘数据的道路（访问控制）或者是的攻击者获得的数据变得不可用（加密技术）来实现。

 # 匿名化技术

通过抽象和压缩技术，以数据的可用性为代价，换取隐私信息的安全性，其过程是原本不同的 QI 属性值变成相同值。达到匿名化的目的。

 # 假名化技术

通过用一个或多个人工标识符或假名来替换数据记录中的大多数标识字段来增强私密性。一个被替换字段的集合可以有一个假名，或者每个被替换字段都可以有一个假名。

 # 去标识化技术

去标识化是指通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别或者关联个人信息主体的过程。去标识化建立在个体基础之上，去除标识符与个人信息主体之间的关联性，保留了个体颗粒度的手段，采用假名、加密、哈希函数等技术。[39]

4.2.3 技术：隐私计算技术

■ 基本概念

隐私计算是指在保护数据本身不对外泄露的前提下实现数据分析计算的一类信息技术，是数据科学、密码学、人工智能等多种技术体系的交叉融合。

■ 主要实现

从技术实现原理上看，隐私计算主要分为密码学和可信硬件两大领域。密码学技术目前以多方安全计算等技术为代表；可信硬件领域则主要指可信执行环境；此外，还包括基于以上两种技术路径衍生出的联邦学习等相关应用技术。

4.2.3.1 扩展技术：可信计算

■ 基本概念

可信计算，其核心目标是保证系统与应用的完整性，从而确保系统或者软件运行在设计目标期望的可信状态。基本思想是在计算机系统中，建立一个信任根，

从信任根开始，到硬件平台、操作系统、应用软件，逐级度量，把这种信任扩展到整个计算机系统，并采取防护措施，确保计算资源的数据完整性和行为的预期性，从而提高计算机系统的可信性。

■ 主要实现

可信计算研究涵盖硬件、软件以及网络等不同技术层面，主要实现方式包括信任根、可信平台模块等衍生技术。

 # 信任根

信任根是可信计算的根基，也是实施安全控制的起点。国际权威组织 TCG（Trusted Computing Group）定义的信任根包括三个，一是可信度量根（RTM），负责完整性度量；二是可信报告根（RTR），负责报告信任根；三是可信存储根（RTS），负责存储信任根。信任根的核心功能是对可信软件栈进行度量和验证，以确保可信。

 # 可信平台模块

可信平台模块是可信计算平台信任根的一部分，本身是一个 SOC 安全芯片，由 CPU、存储器、I/O、密码协处理器、随机数产生器和嵌入式操作系统等部件组成。SOC 安全芯片具有密码运算和存储能力，能提供密钥生成和公钥签名等功能，内部带有非易失性存储器，能永久保存用户身份信息或秘密信息。

 # 信任链传递技术

在可信计算机系统中，信任链被用于描述系统的可信性，信任链传递技术便适用于该场景。整个系统的信任链传递是指，从信任根开始，到平台加电 BIOS

执行，再到操作系统加载程序执行，最后到操作系统启动、应用程序执行的一系列过程。信任链一直从信任根处层层传递上来，从而保证该终端的计算环境始终是可信的。

 # 可信 BIOS 技术

可信 BIOS 技术直接对计算机系统中的输入、输出设备进行硬件级控制，是连接软件程序和硬件设备之间的枢纽，主要负责机器加电后各种硬件设备的检测初始化、操作系统装载引导、中断服务提供及系统参数设置等操作。在高可信计算机中，BIOS 和安全芯片共同构成系统的物理信任根。

 # 可信计算软件栈技术

可信计算软件栈是可信计算平台的支撑技术，用来向其它软件提供使用安全芯片的接口，并通过实现安全机制来增强操作系统和应用程序的安全性。可信计算软件栈通过构造层次结构的安全可信协议栈创建信任，提供基本数据的私密性保护、平台识别和认证等功能。

 # 可信网络连接技术

可信网络连接技术主要解决网络环境中终端主机的可信接入问题，在主机接入网络之前，必须检查其是否符合该网络的接入策略，可疑或有问题的主机将被隔离或限制网络接入，直到经修改或采取相应的安全措施为止。

4.2.3.2 扩展技术：密码学应用

■ 基本概念

密码学应用，是指基于密码学，与人工智能、区块链等学科技术交叉融合，实现面向隐私信息全生命周期保护的计算理论和方法,目的是在保障数据本身不对外泄露的前提下实现数据分析计算。

■ 主要实现

隐私计算中有很多融合了密码学的子技术应用，例如安全多方计算、同态加密、零知识证明、联邦学习等技术。

 # 安全多方计算

安全多方计算（ Secure Multi-party Computation, MPC 或 SMPC），是一种分布式计算和加密方法，主要研究的是在无可信第三方的情况下，如何安全的计算一个约定函数的问题。安全多方计算允许多个参与方在使用机密数据时数据不出门，可用不可见。安全多方计算技术核心思想是设计特殊的加密算法和协议，从而实现利用加密数据直接进行计算，获得计算结果，同时不知道数据明文内容。

 # 同态加密

同态加密（Homomorphic Encryption），即通过利用具有同态性质的加密函数，对加密数据进行运算，同时保护数据的安全性。同态加密允许对密文处理后仍然是加密的结果，即对密文直接进行处理，跟对明文进行处理后再对处理结果加密，得到的结果相同，从抽象代数的角度讲，保持了同态性。同态加密对于数据安全来讲，更关注于数据的处理安全，并提供了一种对加密数据处理的功能，处理过程无法得知原始内容，同时数据经过操作后还能够解密得到处理好的结果。

 # 零知识证明

零知识证明，即：证明者（prover）有可能在不透露具体数据的情况下让验证者（verifier）相信数据的真实性。零知识证明可以是交互式的，即证明者面对每个验证者都要证明一次数据的真实性；也可以是非交互式的，即证明者创建一份证明，任何使用这份证明的人都可以进行验证。零知识证明目前有多种实现方式，如 zk-SNARKS、zk-STARKS、PLONK 以及 Bulletproofs。每种方式在证明大小、证明者时间以及验证时间上都有自己的优缺点。

 # 联邦学习

联邦学习，其本质是分布式的机器学习，在保证数据隐私安全的基础上，实现共同建模，以提升模型的效果。联邦学习的目标是在不聚合参与方原始数据的前提下，实现保护终端数据隐私的联合建模。根据数据集类型不同，联邦学习分为横向联邦学习、纵向联邦学习与联邦迁移学习。

4.2.3.3 扩展技术：差分隐私

■ 基本概念

差分隐私旨在提供一种当从统计数据库查询时，可以最大化数据查询准确性，同时最大限度减少识别其记录的机会。差分隐私有两个重要特性，一是差分隐私会假设攻击者能获得目标记录以外的所有其他信息;二是差分隐私是一种建立在严格的数学定义之上的可量化评估的方法。

■ 主要实现

差分隐私的实现方式，可通过加适量的干扰噪声来实现，目前常用的添加噪音的机制有拉普拉斯机制和指数机制，其中拉普拉斯机制用于保护数值型的结果，指数机制用于保护离散型的结果。

4.2.4 技术：身份认证技术

■ 基本概念

身份认证技术，是指对实体和其所声称的身份之间的绑定关系进行充分确认的过程，目的是为了解决网络通信双方身份信息是否真实的问题，使各种信息交流可以在一个安全的环境中进行。身份认证技术可以提供关于某个人或某个事物身份的保证，这意味着当某人（或某事）声称具有一个身份时，认证技术将提供某种方法来证实这一声明是正确的。

■ 主要实现

在网络安全，乃至数据安全中，身份认证技术作为第一道，也是极其重要的一道防线，有着重要地位。可靠的身份认证技术可以确保信息只被正确的“人”访问。身份认证技术的发展，经历了从软件实现到硬件实现，从单因子认证到多因子认证，从静态认证到动态认证的过程。目前比较流行的身份认证技术包括口令认证技术、无口令认证、生物特征认证等。

4.2.4.1 扩展技术：口令认证技术

■ 基本概念

口令认证技术[40]是基于知识证明的身份认证机制中最常用的技术。系统为每一个合法用户建立一个用户名/口令对，当用户登录系统或使用某项功能时，系

统对用户输入的用户名、口令进行验证。口令认证系统有密码算法抗攻击能力强、兼容性好、使用方便可靠等显著特点。

■ 主要实现

口令认证技术的实现，根据验证口令的产生方式的不同，口令认证可以分为静态口令认证、一次性口令认证和双因素动态口令认证等种类。

 # 静态口令认证

静态口令认证是指用户登录系统在进行身份认证的过程中，提交给系统的验证数据是固定不变的。静态口令认证主要用于一些比较简单的系统或安全性要求不高的系统，例如：PC 机的开机口令、Unix 系统中用户的登录、Windows 用户的登录、电话银行查询系统的帐户口令等。

 # 一次性口令认证

一次性动态口令认证也称动态口令认证，其机制是产生验证信息的过程中加入不定因素，使每次登录过程中网络传送的数据包都不同，以此来提高登录的安全性。不定因子可以是用户登录的时间或者用户登录的次数等。

 # 双因素动态口令认证

双因素动态口令认证机制，是在静态口令认证的基础上，增加一个物理因素，并在登录过程中增加不确定的变化因素以生成动态变化的验证信息。其认证流程如下：用户在业务终端上登录时输入用户身份 ID 和静态口 PW；业务终端通过专用设备将第二个物理认证因素上的数据读入；业务终端将对静态口令和第二个物理因素数据进行密码处理得到动态的验证口令，然后将动态验

证口令送到中心主机进行验证。中心主机系统将验证口令数据包解密后，进行安全认证。业务终端接收中心主机返回的认证结果，并根据结果决定用户的操作。最常见的物理因素有：生物特征和智能卡。智能卡与静态口令结合使用的认证方式也是目前应用最广泛的双因素动态口令认证机制。

4.2.4.2 扩展技术：无口令认证

■ 基本概念

无口令认证，是指使用密码以外的其他内容验证用户身份的过程。无口令认证通过消除密码管理过程以降低威胁媒介风险来增强安全性,是身份和访问管理的新兴子领域。

■ 主要实现

无口令认证的主要实现原理是，用户选择一个本地的认证方案（例如按一下指纹、看一下摄像头、对麦克说话，输入一个 PIN 等）把他的设备注册到在线服务上去，也就是说只需一次注册，之后用户再需要认证时，只需简单重复一个认证动作即可，即：无需通过物理媒介来登录。

4.2.4.3 扩展技术：生物特征认证

■ 基本概念

生物特征认证，是指通过计算机与光学、声学、生物传感器和生物统计学原理等高科技手段密切结合，利用人体固有的生理特性（如指纹、脸象、虹膜等）和行为特征（如笔迹、声音、步态等）来进行个人身份的鉴定。

■ 主要实现

生物特征技术是目前最为方便和安全的识别技术，实现方式包括人脸识别、指纹识别、虹膜识别、掌静脉识别、声纹识别等技术。

人脸识别技术

人脸识别技术，是指能够识别或验证图像或视频中的主体的身份的技术。人脸识别系统通常由人脸检测、人脸对齐、人脸表征、人脸匹配等模块构成。高精度的人脸识别系统需要针对人脸识别的挑战因素如光照、姿态、遮挡等进行针对性地设计。比如针对光照和姿态因素，可以在收集训练样本时力求做到每个个体覆盖足够多的光照和姿态变化，或者通过有效的预处理方法以补偿光照和姿态带来的人脸身份信息变化。

指纹识别技术

将识别对象的指纹进行分类比对从而进行判别的技术。一个典型的指纹识别系统包括：指纹识别 Sensor+特征提取/匹配模块+特征模板库+应用软件。指纹的匹配可分为两步，首先是提取待验证的指纹的特征，然后将其和指纹模板库中的模板指纹进行相似度比较，从而判断两个指纹图像是否来自同一主体。

虹膜识别技术

虹膜识别技术，是指基于眼睛中的虹膜特征进行身份识别的技术。虹膜识别技术一般包括四个步骤，分别是虹膜图像获取、图像预处理、特征提取和特征匹配。虹膜代码（Iris Code）通过复杂的运算获得，可以提供数量较多的特征点。

掌静脉识别技术

静脉识别技术，是指基于掌静脉分布特征进行身份识别的技术。掌静脉识别实现需要四个步骤，第一，利用对人体安全的近红外光照射手掌获取图像，将数字图像存贮在计算机系统中；第二，图像校正：对掌静脉图像的位置和角度进行调整，使其符合特征提取要求；第三，特征提取：提取静脉分布特征，获取特征图；第四，图像对比匹配：将特征图与数据库中的原始模板进行比较，计算相关性，如果匹配则成功识别身份，不匹配则识别失败。

声纹识别技术

声纹识别技术，是指通过语音信号提取代表说话人身份的相关特征（如反映声门开合频率的基频特征、反映口腔大小形状及声道长度的频谱特征等），进而识别出说话人身份等工作方面的技术。基本原理是针对每一个说话人建立一个能够描述这一说话人个性特征的模型，作为此说话人个性特征的描述，并进行特征匹配判断。

4.2.4.4 扩展技术：令牌

- 基本概念

令牌，是指在计算机和网络中用于访问系统、声明权限的字符串凭证。

- 主要实现

令牌是身份认证技术中的一种重要子技术应用，实现方式主要包括 X.509 证书管理、PKI 技术、RFIS 身份认证等。

X.509 证书管理

X.509 证书管理，是指为实现系统业务数据传输和交换过程中的真实性、完整性和不可抵赖性，保障系统交易安全，支付系统与其参与者之间采用基于公钥基础设施(Public Key Infrastructure，简称 PKI)的电子签名机制，使用第三方认证机构发放的数字证书提供安全认证服务，支持证书格式 X.509 标准，并通过相关技术工具自动颁发、更新以及管理证书，从而提高安全性和高效性的一个过程。

PKI 技术

PKI（Public Key Infrastructure），即“公开密钥体系”，是一种遵循既定标准的密钥管理平台，它能够为所有网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系，简单来说，PKI 是利用公钥理论和技术建立的提供安全服务的基础设施。PKI 的基础技术主要包括加密、数字签名、数据完整性机制、数字信封、双重数字签名等。

RFIS 身份认证

RFIS(Radio Frequency Identification，射频识别)身份认证，是指基于射频识别技术而实现身份认证的过程。可通过无线电讯号识别特定目标并读写相关数据，而无需识别系统与特定目标之间建立机械或光学接触。RFIS 身份认证系统包括射频标签和读写器两部分，射频标签是承载识别身份特征信息的载体，读写器是获取身份特征信息的装置。射频识别的标签与读写器之间利用感应、无线电波或微波，进行双向通信，实现标签存储身份特征信息的识别和数据交换，从而达到身份认证识别的目的。

4.2.4.5 扩展技术：机器 ID 管理

组织或企业中的机器身份(ID)[15]的数量日益增加，这要求从业者进一步把机器身份管理作为组织或企业安全策略中重要组成。

■ 基本概念

机器 ID 管理，是指为与其他实体（如设备、应用、云服务或网关）交互的机器建立和管理身份信任。

■ 主要实现

机器 ID 可以快速无误地完成任务来提高生产力，但广泛应用让可见性获得和最低权限访问强制执行变得更困难，因此需要保护机器 ID 和实施机密治理。如果在多云环境中想要降低机器 ID 管理风险，可以通过：对所有用户(人类和非人类)使用即时(JIT) 权限访问、保持零持续权限(ZSP)、集中和扩展权限管理、通过高级数据分析(ADA)获得统一访问可见性、将机密治理构建到持续集成(CI)/持续交付(CD)流程中等技术手段实现。

4.2.4.6 扩展技术：去中心化身份（DID）

■ 基本概念

去中心化身份（DID,Decentralized identifiers），是一种新型标识符，是可实现可验证的去中心化数字身份。这是一个新的全局唯一标识符的类型，目的是使个人和组织使用信任的系统生成自己的标识符，和传统标识符不同，去中心化标识符和中心化的身份注册机构、身份提供商以及证书权威中心等传统中心化机构解耦，去中心化标识符的控制人（或所有者）可以直接控制去中心化标识符，而无需任何第三方的许可。

[15] 比如：物联网设备、虚拟机、容器和 RPA 机器人等机器 ID。

■ 主要实现

去中心化身份（DID）由三部分组成：代表去中心化标识符的识别字符串：did；每个 DID 方案不同的识别符；该 DID 方案中实体的识别符。该技术可以用来标识任何实体，包括个人、机构、组织、关系以及事物等，包括“人、财、物、事”等不同实体，主要实现方式包括区块链等技术。

4.2.5 技术：访问控制技术

■ 基本概念

访问控制（Access Control）指系统对用户身份及其所属的预先定义的策略组限制其使用数据资源能力的手段。通常用于系统管理员控制用户对服务器、目录、文件等网络资源的访问。访问控制的主要目的是限制访问主体对客体的访问，从而保障数据资源在合法范围内得以有效使用和管理。

■ 主要实现

访问控制的功能性实现一般需要两步：一是识别和确认访问系统的用户；二是利用技术手段决定该用户可以对某一系统资源进行何种类型及权限的访问。技术实现方式可分为网络访问控制、权限管理控制、风险操作控制和数据访问控制等衍生技术。

4.2.5.1 扩展技术：网络访问控制

■ 基本概念

网络访问控制，是指基于网络安全的保证网络数据资源不被非法使用和访问的技术，也是保证网络安全的核心技术之一。该技术明确地定义和限制了信息系

统用户能够对资源执行的访问操作,从而有效提供了对信息资源的机密性和完整性的保护。

■ 主要实现

在网络安全的大背景下，网络访问控制作为一种重要的安全支撑技术得到广泛应用，主要实现手段包括了入网访问控制、网络权限控制、目录级安全控制、属性安全控制、服务器安全控制等技术。

 # 入网访问控制

通过控制能够登录服务器并获取网络资源的用户，以及控制准许用户入网的时间和准许用户入网工作站的方式，为网络访问提供第一层访问控制。用户的入网访问可分为三个步骤:用户名的识别与验证、用户口令的识别与验证、用户账号的缺省限制检查。三道关卡中只要任何一关未过，该用户便不能进入该网络。

 # 网络权限控制

网络权限控制，是指通过控制用户和用户组访问目录、子目录、文件和其他资源的权限，实现减少网络非法操作的一种安全保护措施。技术实现方式可分为受托者指派和继承权限屏蔽（IRM）等，受托者指派控制用户和用户组如何使用网络服务器的目录、文件和设备。继承权限屏蔽相当于一个过滤器，可以限制子目录从父目录那里继承哪些权限。

 # 目录级安全控制

目录级安全控制，是指通过指定用户在目录一级的权限，实现网络安全控制的技术手段。网络管理员为用户指定适当的访问权限，这些访问权限控制着用户对服务器的访问。多种访问权限的有效组合可以让用户有效地完成工作，同时又能有效地控制用户对服务器资源的访问，从而加强网络和服务器的安全性。

 # 属性安全控制

属性安全控制，是指通过给文件、目录等指定访问属性的方式，保护网络数据安全的一种技术手段。首先对网络数据资源标出一组安全属性，然后根据用户对网络资源的访问权限建立一张访问控制表，从而表明和落实用户对网络资源的访问能力和权限，属性设置可以覆盖已指定的任何受托者指派和有效权限。

 # 服务器安全控制

服务器安全控制，是指通过设置口令锁定服务器控制台，以及设定服务器登录时间限制、非法访问者检测和关闭的时间间隔等方式，以防止非法用户修改、删除重要信息或破坏数据的安全手段。

4.2.5.2 扩展技术：权限管理控制

■ 基本概念

权限管理控制，是指针对不同用户的访问资源进行权限的控制，避免因权限控制缺失或操作不当而引发各种风险问题，如操作错误，隐私数据泄露等问题。

■ 主要实现

权限控制可以说是整个系统中最基础的组成部分之一，同时也是很复杂的技术。在实际项目中会遇到多个系统、多个用户类型以及多个使用场景，这需要具体问题具体分析，目前比较主流的权限控制实现方式包括 DAC、MAC、RBAC、ABAC 等技术。

DAC

DAC（Discretionary Access Control），即：自主访问控制。DAC 模型是通过建立客体关联表，主要通过访问控制列表的形式将主体和客体的关联性在表中组织起来。其自主性主要体现在系统中的主体可以将其拥有的权限授权给其他主体而不需要经过系统安全员的允许。即用户有权对自身所创建的访问对象（服务器、目录、文件、数据等）进行访问，并可将对这些对象的访问权授予其他用户、系统，以及从授予权限的用户、系统收回访问权限。DAC 模型的优点是比较灵活，易于实现；缺点是资源管理比较分散，主体间的关系不能在系统中明显体现出来，且易造成权限传递失控，导致信息泄露，此外，如果主体、客体数量庞大，会带来极大的系统开销，因此很少被应用于大型系统。

MAC

MAC（Mandatory Access Control），即：强制访问控制。MAC 的基本思想是依据主体和客体的安全属性的级别来决定主体是否拥有对客体的访问权限，主要用于多层次安全级别的系统。MAC 机制下，系统内每一个用户或主体都被赋予一个安全属性，用来表示能够访问客体的敏感程度。同样地，每一个客体也被赋予一个安全属性，以反映本身的敏感程度。系统通过比较主体和

客体相应的安全属性的级别来决定是否授予一个主体对客体的访问请求。MAC 机制下的安全属性由系统策略管理员分配，具有强制性，用户或用户进程不能改变自身或其它主、客体的安全属性。MAC 模型的优点是拥有较高安全性，能够通过信息的单向流动来防止机密信息的泄露，而且由于用户不能改变自身或者其他客体的属性，可以防止用户滥用职权；缺点则是灵活性较低，权限不能实现动态变化，授权管理比较困难，难以防御用户恶意泄露信息。

RBAC

RBAC（Role-Based Access Control），即：基于角色的访问控制。为解决 DAC 和 MAC 将权限直接分配给主体，易造成管理困难的缺陷，于是在访问控制模型中引入了“角色”的概念，即 RBAC。角色是指一个或一群用户在组织内可进行的操作的集合。RBAC 通过引入角色这一中介，可以实现对角色权限的更改将自动更新拥有该角色的每个用户的权限，如果用户改变角色，权限也相应发生变化。RBAC 优点是实现了用户和权限的逻辑分离，从而简化授权管理，实现最小权限原则；缺点是，同一个用户可以同时激活多个角色，约束粒度较大，易造成用户权限过大带来安全隐患，主客体之间联系较弱，可扩展性不强，难以适用于分布式系统。

ABAC

ABAC（Attribute-Based Access Control），即：基于属性的访问控制，它是一种细粒度的访问管理方法，并基于已分配给用户、操作、资源或环境的已定义规则，决定批准或拒绝对特定信息的访问请求。ABAC 针对复杂信息系统

中细粒度访问控制和大规模用户动态扩展问题，将实体属性（组）的概念贯穿于访问控制策略、模型和实现机制三个层次，并通过主体、客体、权限和环境属性的统一建模，进行描述授权和访问控制约束，使其具有足够的灵活性和可扩展性。ABAC 模型的优点是框架式的，可与其他访问控制模型结合（如 RBAC）；缺点是所有要素均需要以属性形式进行描述，但一些关系用基本的属性不易描述。

4.2.5.3 扩展技术：风险操作控制

- 基本概念

风险操作控制是指运用安全技术控制数据安全风险，并适用于各类场景的一系列操作或产品。

- 主要实现

风险操作控制技术目前实现于系统和设备指令级的典型产品是堡垒机，实现于应用和业务级的典型产品是 WAF（Web 应用防火墙）。

 # 系统和设备指令级

系统和设备指令级的典型产品是堡垒机，堡垒机是指在特定网络环境下，为保障网络和数据不受外部和内部用户入侵及破坏，而运用各类技术手段监控及记录运维人员对网络内服务器、网络设备、安全设备、数据库等设备的操作行为，以便报警、处理及审计定责的运维审计系统。堡垒机的设计来源于 4A 理念，即认证（Authen）、授权（Authorize）、账号（Account）、审计（Audit）。

应用和业务级

应用和业务级的风险操作控制产品主要是 WAF（Web Application Firewall），即 Web 应用防火墙，主要指通过执行一系列针对 HTTP/HTTPS 的安全策略来专门为 Web 应用提供保护的一款产品，主要分为云 WAF、硬 WAF、软 WAF 三种。

4.2.5.4 扩展技术：数据访问控制

■ 基本概念

数据访问控制，是指基于数据的，适用于不同场景的身份验证和权限管理技术体系，目的是确保用户数据不被越权访问及利用。

■ 主要实现

数据访问控制是保障数据安全的重要手段，主要实现方式包括存储介质访问控制和网间数据摆渡等技术手段。

存储介质访问控制

存储介质访问控制，是指针对于存储数据载体（比如软盘、光盘、DVD、硬盘、闪存、U 盘、CF 卡、SD 卡、MMC 卡、SM 卡、记忆棒（Memory Stick）、xD 卡等）而建立的一套身份验证和权限管理机制，从而实现存储介质中数据的安全防护。存储介质访问控制的实现方式包括了端口管控、介质加密等技术。

网间数据摆渡

网间数据摆渡是指当摆渡系统与内网联通时，与外网是断开状态；当摆渡系统与外网联通时，与内网是断开状态，目的是在确保网络安全隔离的前提下，进行适度的信息数据交换，目前基于该技术的应用产品是网闸。

4.2.6 技术：数字签名技术

■ 基本概念

数字签名（Digital S ignature），签名者使用私钥对待签名数据的杂凑值做密码运算得到的结果，该结果只能用签名者的公钥进行验证，用于确认签名数据的完整性、签名者身份的真实性和签名行为的抗抵赖性。【来源：GM/Z 4001-2013,2.113】[41]

■ 主要实现

数字签名使用了公钥加密领域的技术实现，用于鉴别数字信息。一套数字签名通常定义两种互补的运算，一个用于签名，另一个用于验证。每种公钥加密体系都能设计实现相应的数字签名，代表性的有 RSA 签名和 DSA 签名。

4.2.6.1 扩展技术：数字证书

■ 基本概念

数字证书（digital certificate），也称公钥证书，由证书认证机构（CA）签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。[42]

■ 主要实现

数字证技术能够保证网上信息传输双方的身份验证和信息传输安全,按类别可分为个人证书、机构证书和设备证书，按用途可分为签名证书和加密证书。

4.2.6.2 扩展技术：签名验签

■ 基本概念

签名验签原理是加密 SDK 通过非对称类型用户密钥提供签名、验签功能，支持 RSA、ECC 和 SM2 非对称密钥算法。签名验签过程：首先，签名者将验签公钥分发给消息接收者；其次，签名者使用签名私钥，对数据产生签名；再次，签名者将数据以及签名传递给消息接收者；最后，消息接收者获得数据和签名后，使用公钥针对数据验证签名的合法性。

■ 主要实现

签名验签技术可为网上各类应用系统的关键数据提供基于数字证书基础上的数字签名服务和签名验签服务，可以广泛应用于网上银行、网上证券和网上支付等电子政务、电子商务中，保证关键业务在交易过程中的信息完整性、不可否认性和事后可追溯性。

4.2.6.3 扩展技术：电子签章

电子签章是电子签名的一种表现形式，利用图像处理技术将电子签名操作转化为与纸质文件盖章操作相同的可视效果,同时利用电子签名技术保障电子信息的真实性和完整性以及签名人的不可否认性。

■ 基本概念

电子签章指使用电子签署电子文件的过程。

■ 主要实现

电子签章将传统印章与电子签名技术进行结合，通过采用组件技术、PKI 技术、图像处理技术以及密码技术，按照公钥密码技术标准体系，以电子形式对电子文档进行数字签名及签章。应用于常见的各类企业的劳动合同、产品购销合同、供应商合同以及企业内部日常的审批等。[43]

4.2.7 技术：DLP 技术

数据（泄露）防护（Data leakage prevention, DLP），又称为“数据丢失防护”(Data Loss prevention, DLP)，通过一定的技术手段，防止企业的指定数据或信息资产以违反安全策略规定的形式流出企业的一种策略。DLP 这一概念来源于国外，是国际上最主流的信息安全和数据防护手段。

■ 基本概念

DLP 技术，即数据泄露防护技术，主要核心是通过识别结构化数据和非结构化等数据资产，根据安全策略执行相关动作，以实现数据资产保护。

■ 主要实现

DLP 技术的内容识别方法别包括关键字、正则表达式、文档指纹、向量学习等；策略包括拦截、提醒、记录等。DLP 技术可部署在终端、电子邮件、云和网络等各种出口通道上，能够为其提供 DLP 功能的工具包括邮件安全和邮件网关（SEG）解决方案、Web 安全网关（SWG）、云访问安全代理（CASB）、终端保护平台以及防火墙等。

4.2.7.1 扩展技术：终端 DLP

■ 基本概念

终端 DLP 以机器学习技术为基础，对企业内部数据资产自动分类分级，智能识别、监控数据资产的分布与使用情况，对终端用户违规行为实时监控。

■ 主要实现

终端 DLP 可以应用于办公设备和移动设备,其系统由 4 个组件组成,包括:终端代理程序、管理服务器、数据可视化中心和规则生成系统。

 # 办公设备 DLP

办公设备 DLP 主要依赖于运行于桌面、笔记本电脑、服务器、Windows、Linux、MacOS 的设备上的软件客户端，提供可见性控制，结合使用需求，对数据进行控制。

 # 移动设备 DLP

通过在移动设备生成虚拟安全域等技术，在安全域内运行使用企业应用，保障企业业务和数据的安全性，如防止截屏、防止转发、防复制粘贴、数据传输和存储加密等。在安全域外，应用、数据和设备权限依然归员工自己控制。

4.2.7.2 扩展技术：网络 DLP

■ 基本概念

网络 DLP 利用部署在企业网络内部或出口的网关设备，实时监测经过企业网络的通信数据内容，自动对网络数据文件分类分级，检测、分析并报告企业敏感数据失泄密事件。

■ 主要实现

网络 DLP 系统由 4 个组件组成，包括：网络 DLP 监控网关、DLP 管理服务器、DLP 数据可视化和 DLP 规则生成系统。

4.2.7.3 扩展技术：端点 DLP

端点 DLP 对静态数据和使用中的数据应用保护策略。端点 DLP 被部署在每个受保护的端点上以软件形式运行，此软件与 DLP 策略服务器通信，以更新策略和报告事件。

- 主要实现

端点 DLP 本质上是网络级 DLP 的端点级实现，支持拦截功能，能实现通常网络 DLP 无法达到的防护等级。

4.2.7.4 扩展技术：邮件 DLP

- 基本概念

邮件 DLP 利用部署在企业邮件网络出口的网关设备，实时监测经过企业网络的通信数据内容，自动对邮件数据文件检测、分析并报告企业敏感数据失泄密事件。

- 主要实现

邮件 DLP 集被动审计和主动控制于一体，通过邮件数据分析、敏感数据识别审计、邮件数据脱敏处理、邮件审批管理、阻断策略响应访问控制等，实现邮件数据传输过程中的安全保障。

4.2.7.5 扩展技术：DLP 集成

- 基本概念

DLP 集成指基于 DLP 的一组技术集合组成的解决方案，可支持根据既定的策略对敏感信息的检测和使用情况提供日志、标记、加密、权限控制和阻断等操作。

■ 主要实现

DLP 集成是一个包含管理平台、网络监控、网络保护、邮件保护、终端保护、数据发现及应用系统保护等多个 DLP 产品的集成套件，能够通过深度内容分析和事务安全关联分析来识别、监视和保护静止、移动和使用中的数据，并联动其它传统安全产品形成整体数据安全解决方案。

 # 企业 DLP 套件

将多个 DLP 集成统一到企业级系统之中，对外传数据内容智能深度识别，防止敏感信息外泄自动发现、梳理并识别企事业单位存储设施内的敏感数据内容，并能对所有发现的敏感数据计算其数据指纹，针对性制定不同密级、不同类型的敏感数据监管和保护策略，智能化防止敏感信息的外泄。

4.2.7.6 扩展技术：数据交换 DLP

数据共享与交换是数据变现、增值最直接通道，同时也是各类违规操作和安全攻击管控难点。

■ 基本概念

数据交换 DLP 指在数据共享交换环节，进行数据防泄露监测。

■ 主要实现

常见的交换 DLP 包含行为追溯和业务分析两部分。

 # 行为追溯

对数据交换行为及用户操作记录进行细粒度审计，通过综合查询为事后溯源提供依据。

 # 业务分析

通过统计分析功能可以详细了解业务运行情况，根据当前业务需求适时调整交换策略。

4.2.7.7 扩展技术：CASB DLP

■ 基本概念

CASB DLP 通过 ICAP 或 RESTful API 集成在本地运行并与企业 DLP 产品结合运行。一些 CASB 提供在云服务中的字段和文件级别加密、标记或编辑内容的能力。但是因为 SaaS 应用程序之外的加密和标记化会影响功能，所以不常使用 CASB 促进的加密和标记化。

■ 主要实现

CASB 能够实施以数据为中心的安全策略，以防止基于数据分类、数据发现以及因监控敏感数据访问或提升权限等用户活动而进行有害活动，通常是通过审计、警报、阻止、隔离、删除和只读等控制措施来实施策略。[44]

4.2.7.8 扩展技术：云原生 DLP

■ 基本概念

云原生 DLP 是将本地部署的 DLP 解决方案整体迁移至云上，解决远程办公场所和移动终端设备的敏感数据保护的问题，从而减少用户需要购置多台 DLP 硬件设备产生的额外费用。

- 主要实现

云原生 DLP 解决方案，通过确保敏感数据在未经加密的情况下不会进入云，并且仅发送到授权的云应用程序，从而专门保护已采用云存储的组织。大多数云 DLP 解决方案会在将文件共享到云之前删除或更改机密或敏感数据，以确保数据在传输和云存储时受到保护。

4.2.8 技术：数据销毁技术

- 基本概念

数据销毁是指将数据存储介质上的数据不可逆地删除或将介质永久销毁，从而使数据不可恢复、还原的过程。

- 主要实现

数据销毁作为数据生命周期中的最后一环，其目的是使得被删除的敏感数据不留踪迹、不可恢复，主要分为硬销毁和软销毁。

4.2.8.1 扩展技术：硬销毁

- 基本概念

数据硬销毁是指从根本上破坏掉存在涉密信息的物理载体，使其失去信息存储能力，是可以非常彻底地解决数据泄露问题的销毁办法。

- 主要实现

数据硬销毁可分为物理销毁和化学销毁两种方式。其中，物理销毁又可分为消磁，及熔炉中焚化、熔炼，借助外力粉碎，研磨磁盘表面等物理破坏方法；化学销毁一般是使用化学药剂对磁盘磁介质进行腐蚀破坏，以达到销毁数据的目的。

 # 消磁

其工作原理是磁性存储设备暴露在消磁器的强大磁场中，以磁性方式破坏存储的数据。硬盘盘面上的磁性颗粒沿磁道方向排列，不同的N/S极连接方向分别代表数据0或1。对硬盘瞬间加强磁场，磁性颗粒就会沿场强方向一致排列，变成清一色的0或者1，失去了数据记录的功能。遭受消磁的设备无法再次重复使用以存储数据。

 # 物理破坏

在这种类型中，数字存储介质（如硬盘驱动器、存储棒、磁带、CD、DVD和Blu-ray光盘、信用卡）会被物理破坏以避免恢复。这种技术通常在情报机构和商业组织中使用，以确保安全处置存储设备并避免可能的分类数据恢复。用于摧毁这些设备的设备称为“硬盘粉碎机和驱逐舰”。

 # 化学腐蚀

即通过利用酸性试剂对存储介质的盘面进行腐蚀，通过破坏盘面的方式避免数据还原，常见有滴盐酸法。如今，生产厂家为了提高介质盘片的耐磨性，会在盘面镀合金薄膜，使得盘片具有抗腐蚀性，导致化学腐蚀法的效果越来越差。

4.2.8.2 扩展技术：软销毁

■ 基本概念

数据软销毁一般是指逻辑销毁，即通过软件方法如数据覆盖等销毁数据。[45]

■ 主要实现

软销毁主要包括格式化、磁盘分区、数据覆写、文件粉碎软件、云资源再分配、等。软销毁的主要优点是不损坏存储设备，操作简单方便，适用范围广。缺点是销毁处理速度慢，覆写次数少时，数据销毁不彻底，销毁的数据依然有可能会被还原。[46]

 # 格式化

对磁盘或磁盘中的分区进行初始化的一种操作，结果是让现有磁盘或分区中的所有文件被清除。格式化分为低级格式化（物理格式化）和高级格式化（逻辑格式化）。低级格式化，是指对磁盘的物理表面进行处理，在磁盘上建立标准的磁盘记录格式，划分磁道和扇区，低级格式化会减少硬盘寿命。高级格式化，是指根据用户指定的文件系统，在磁盘的特定区域写入特定数据，以达到初始化磁盘等目的的一个操作。

 # 磁盘分区

将一个实体磁盘驱动器分为数个分区，将要销毁的关键数据放到较小的分区中，进行应急销毁，无关数据放到较大的分区中，不进行销毁。

 # 数据覆写

将非涉密信息写入已经存在敏感信息的硬盘簇的过程。该硬盘存有的信息均是以二进制的“1”和“0”模式储存的。应用先前认定的无意义、无价值、无规律的数据多次覆盖在硬盘上，那么就无法得知存储介质上的信息是“1”还是“0”，如此，销毁存储介质上的信息的目的也就达到了。数据覆写法是最经济、较安全的数据软销毁方式，适用于密级要求不是很高的信息设备，处理后的硬盘还可以继续使用，尤其是需要对某一特定文件进行销毁而不能对其他文件进行破坏时，这种方法则更为可取。

 # 文件粉碎软件

粉碎工具软件所具有的文件粉碎功能，大多没有通过专门机构的认证，用于处理带有密级的数据，其可信度和安全性都不高。

 # 云资源再分配

当云硬盘不再使用且已备份重要数据时，可以通过销毁云硬盘来释放虚拟资源，实现再分配。销毁云硬盘时，会同时删除云硬盘中所有数据且不可找回，已经销毁的云硬盘不可恢复。云硬盘包括非弹性云硬盘和弹性云硬盘。其中，非弹性云硬盘的生命周期跟随云服务器，只能在云服务器销毁时被销毁；弹性云硬盘的生命周期独立于云服务器，因此可以独立于云服务器而销毁，销毁方式包括手动销毁和自动销毁。

4.2.8.3 扩展技术：销毁审计

- 基本概念

利用安全审计方法论，设计审计原则，对介质销毁安全管理岗位人员、销毁业务的实际落地执行性进行确认。

■ 主要实现

可通过内部审计、外部审计等形式以调研访谈、问卷调查、流程观察、文件调阅、技术检测等多种方式实现。

4.2.9 技术：云数据保护技术

■ 基本概念

数据保护技术是指利用云资源和虚拟化技术，实现云平台海量数据的保护技术。通常包含数据分级存储、多租户身份认证等。

■ 主要实现

在数据安全领域，云安全保护技术呈现“百花齐放”，基于报告篇幅问题，本文重点探讨云密码服务、云身份鉴别服务、云身份管理和访问控制等已经在非云领域得到算法分析、模型推导等充分验证的安全技术。

4.2.9.1 扩展技术：云密码服务

■ 基本概念

云密码服务是云平台通过资源池化技术整合底层密码设备资源（云计算密码资源和密码应用基础设施），从而提供足够的密码服务支撑能力，为云租户提供基于API、密码中间件等方式的密码资源调用能力。

■ 主要实现

云密码服务将密码服务与云计算平台进行结合，通过调度加密机集群动态扩充密码运算能力，使密码运算速度大大提高，系统稳定性得到极大增强，更好的为用户提供集中化、虚拟化、透明化的密码运算服务。根据云计算中的密码应用需求，云密码服务可分为三类：云密码资源服务（CryptographyResource as a Service，CRaaS）、云密码功能服务（Cryptography Function as a Service，CFaaS）、云密码业务服务（CryptographyBusiness as a Service， CBaaS）。

 # 密钥管理（KMaaS，Key Management-as-a-Service）

根据安全策略，对密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等密钥全生命周期的管理。

 # 加密即服务（EaaS，Encryption-as-a-Service）

密码服务提供商通过 Web 服务 API 代表终端设备执行密钥加密和解密操作。用于执行这些操作的加密密钥存储在密码服务提供商的密钥管理系统中，终端设备在任何时候都不拥有这些密钥。

 # 基础设施即服务（IaaS）容器加密

企业组织保护由云服务提供商保管的数据的一种方法，其类似笔记本电脑上的硬盘加密，但是运用于来自云端保护的整个进程或应用程序的数据，未来可能成为云提供商提供的一项标配功能。

4.2.9.2 扩展技术：云身份鉴别服务

- 基本概念

云身份鉴别服务是构建在 SaaS 层的云服务，为不同云计算模式的云服务提供身份鉴别服务。

■ 主要实现

作为云安全的第一道门槛，云身份鉴别服务使用的身份鉴别技术是各种安全措施可以正常实施的前提，除了传统的用户名/口令方式，基于智能设备、智能卡、生物识别技术不断出现在新的应用场景中，单点登录、委托鉴别、身份联合、多因素鉴别等鉴别机制也已得到较为成熟的研究。

4.2.9.3 扩展技术：云身份管理和访问控制技术

■ 基本概念

云身份管理和访问控制技术，是基于云计算环境的身份管理和访问控制技术，其定义和管理了云服务用户的身份角色及其所需资源的访问权限，并根据用户身份角色生命周期，对其所需资源访问权限进行动态管理。通常 IAM 会经过认证、授权、访问、数据供应、监控审计等步骤。

■ 主要实现

云身份管理和访问控制技术是保障合理的访问能顺利进行而非法的访问能被拒绝的主要措施，通常会经过认证、授权、访问管理、数据供应、监控审计等步骤。

 # 特权访问管理(PAM，Privileged access management)

管理员或超级用户的一种访问权限，可让上述人士在任何时间、任何地点完全控制关键计算机系统和应用。其中含有一组保护、管理和监视特权访问、用户和凭据的策略、流程和工具。

4.2.10 技术：大数据保护技术

除了传统的网络安全、信息安全、数据安全相关保护技术外，在大数据环境下安全保护技术具有特定应用背景下数据保护技术。

- 基本概念

大数据保护技术指在大数据处理环境下，针对大数据自身安全特性，施加安全增强的数据保护技术。

- 主要实现

常见的大数据保护技术包含数据隔离、分层访问、列数据授权、批量授权等。

 # 数据隔离

在中国墙访问控制模型下，结合业务场景，可以得出针对不同的业务，不同的客户，不同的项目，需要实现数据隔离。利用访问控制手段，实现只能调取某些相关的数据，而无法调取，或者说没有权限其他不相关的数据。

 # 数据分层访问

强制访问控制的现实工程应用，即不同层级业务部门对数据具备不同的访问权限，高层级部门可以访问底层级部门的数据，而低层级部门不可访问高层级部门的数据。

 # 列级数据授权[16]

不同业务部门对同一份数据的访问权限要求不同，所以要求能够对数据进行精细化授权。

 # 批量授权

结合 RBAC 模型和 ABAC 模型，针对大规模用户群体，可在利用批量授权或者基本角色的授权模型，来实现一次授权，相同权限内员工现时赋权。

4.3 D:检测

在检测战术领域，结合数据动态流转特性，本文共收录六类检测手段，即威胁检测、流量监测、数据访问治理[17]、安全审计、共享监控等。

4.3.1 技术：威胁检测

■ 基本概念

威胁检测，是指采用应用威胁情报、机器学习、沙箱、大数据技术计算资产历史行为等多种检测方法，对网络流量和终端进行实时的监控，深度解析、发现与成分分析；对 IT 资产进行精细化识别和重要度评估，帮助信息系统管理者精准检测失陷风险，追溯攻击链，定位攻击阶段，防止攻击进一步破坏系统或窃取数据的主动安全排查行为。

■ 主要实现

[16] 通过 AOE 模型和 ABAC 模型可以很好实现列级数据授权管理。
[17] 本处的数据访问治理与本章节第七部分数据安全治理（战术：治理）用语接近，但考虑本处治理更多针对数据访问过程技术管控，故仍然归类于战术：检测。

通过对全流量常态化威胁监测，提取行为模式和属性特征，创建异常行为基线，智能检测分析如内网横移行为、漏洞利用行为、隐蔽通信行为等 APT 高级威胁攻击行为，提前发现或隐藏在流量和终端日志中的可疑活动与安全威胁因素。

4.3.1.1 扩展技术：APT 检测

- 基本概念

APT[18]监测，是指通过网络流量深度分析实现高级威胁检测和响应，采用大数据处理架构集合机器学习、文件虚拟执行检测技术、攻击行为建模分析等新一代 AI 技术，针对各种网络入侵攻击、恶意代码传播、黑客控制及渗透攻击等，尤其是新型网络攻击、隐蔽黑客控制、APT 攻击等高级网络攻击等技术进行深度攻击威胁挖掘，并进行追踪和定位，提升自身主动预判安全防护能力的监测行为。

- 主要实现

基于未知文件行为检测的方法。一般通过沙箱技术罪恶意程序进行模拟执行，通过对程序的行为分析和评估来判断未知文件是否存在恶意威胁；基于终端应用监控的方法，一般采用文件信誉与黑白名单技术在终端上检测应用和进程；基于大数据分析的方法，通过网络取证，将大数据分析技术和沙箱技术结合全面分析 APT 攻击。

4.3.1.2 扩展技术：欺诈检测

- 基本概念

[18] APT（Advanced Persistent Threat）是指高级持续性威胁，本质是针对性攻击。它是利用先进的攻击手段对特定目标进行长期持续性网络攻击的攻击形式。通常以移动设备、邮件、防火墙和服务器漏洞为目标和攻击对象进而入侵。素材来源于公众号“全栈网络空间安全”文章《APT 攻击检测与防御技术》

欺诈检测[19]，是指利用机器数据和机器学习，搜索、检测和调查数据，通过机器数据中的异常情况来检测和调查异常值，以快速发现例如供应商欺诈、员工费用欺诈、财务报表欺诈、贿赂和资产挪用、减少资金、声誉损失以及组织效率低下等非常规不利现象的数据检测行为。

■ 主要实现

越来越多的行业正在采用机器学习和人工智能以检测和防止欺诈。机器学习算法可以学习并适应所处理的每一个数据，可在打击欺诈方面发挥作用。经过优化的 AI 系统不仅能适应新变化，还能发现新模式而不会产生可能会导致过多假阳性的过拟合。

4.3.2 技术：流量监测

■ 基本概念

网络流量是指单位时间内通过网络设备和传输介质的信息量（报文数、数据包数或字节数）。流量检测，是指针对网络流量以及其他流量进行的检测分析。

■ 主要实现

流量检测需要对网络中传输的实际数据进行分析，包括从底层的数据流一直到应用层的数据的分析，目前包括网络流量分析、高级安全分析、文件分析、TLS 解密等技术。

4.3.2.1 扩展技术：网络流量分析

■ 基本概念

[19] 素材来源于 SPLUNK 官方网站

网络流量[20]分析，是指对在网络中传输的实际数据流进行分析，包括从底层的数据流一直到应用层的数据的逐级分析，也称为网络协议分析。网络流量分析可以对多个资产的攻击告警组合成场景化的攻击事件，进行立体化的呈现，还原攻击链条，确定安全事件的细节，为网络和应用问题的分析、特别是数据包的安全分析提供依据。

图 8 七层通讯协议模型

■ 主要实现

网络的作用是传输应用数据，根据 OSI 协议模型，发送方的应用数据由下层协议逐层处理，最后通过物理层传输，接收方则逐层向上处理从物理链路上接收的信号，最后还原成应用层数据。因此，一个 Web 应用数据在 OSI 模型中的网络数据传输处理过程为：应用数据在应用层采用 HTTP 协议，在传输层被分段，在网络层封包，在数据链路层封帧，由物理层传输，由每一层进行处理，按照相应的协议进行封装。

DPI 深度包检测

[20] 网络流量，是单位时间内通过网络设备或传输介质的信息量(报文数、数据包数或字节数)。

端口识别技术仅分析 IP 包的层 4 以下的内容，包括源地址、目的地址、源端口、目的端口以及协议类型。DPI（深度包检测）除了对前面的层次分析外，还增加了应用层分析，深入读取 IP 包载荷的内容来对协议中的应用层信息进行分析读取，进而识别各类型应用。DPI 是一种基于应用层的流量检测和控制技术，当 IP 数据包、TCP 或 UDP 数据流经过基于 DPI 技术的带宽管理系统时，该系统通过深入读取 IP 包载荷的内容来对 OSI7 层协议中的应用层信息进行重组，从而得到整个应用程序的内容，然后按照系统定义的管理策略对流量进行整形操作。

 # DFI 深度动态流检测

与 DPI 进行应用层的载荷匹配不同，DFI 采用的是一种基于流量行为的应用识别技术，即不同的应用类型体现在会话连接或数据流上的状态各有不同。例如，网上 IP 语音流量体现在流状态上的特征就非常明显：RTP 流的包长相对固定，一般在 130～220byte，连接速率较低，为 20～84kbit/s，同时会话持续时间也相对较长；而基于 P2P 下载应用的流量模型的特点为平均包长都在 450byte 以上、下载时间长、连接速率高、首选传输层协议为 TCP 等。DFI 技术正是基于这一系列流量的行为特征，建立流量特征模型，通过分析会话连接流的包长、连接速率、传输字节量、包与包之间的间隔等信息来与流量模型对比，从而实现鉴别应用类型。

4.3.2.2 扩展技术：高级安全分析

- 基本概念

高级安全分析[47][48][49]是基于网络全流量分析技术，旁路采集、分析和存储所有网络流量，通过威胁情报检测已知威胁，通过回溯分析数据包特征、异常网络行为，发现潜伏的高级未知攻击的行为。

■ 主要实现

可基于网络流的安全分析和异常检测工具，利用最先进的连续流挖掘引擎（Continuous Stream Mining Engine™）技术检测零日网络入侵并对其进行分类，实时检测处理网络安全威胁。

4.3.2.3 扩展技术：文件分析

■ 基本概念

文件分析[50][51]是指运用机器学习、深度学习、知识图谱等技术，进行智能化解析、审查、比对，对以文件形式存贮的数据信息进行分析、评估和审核的行为。

■ 主要实现

对文字进行结构化提取、分析和理解，从语义层面进行关联，精准理解文本含义;深度学习技术在应对复杂文本和非规范用语时,能够快速建模并准确处理;通过知识图谱技术提炼知识的关联结构，构建内容之间深度联系，提供更智能的检索方式，辅助决策意见。

4.3.2.4 扩展技术：TLS流量解密

■ 基本概念

TLS 流量解密[52][53]，是指通过监测应用性能、分析使用模式的方法，识别入站和出站加密流量中的隐藏威胁,避免网络出现数据泄露或遭到使用加密通信的威胁攻击的技术行为。

■ 主要实现

恶意软件会在 TLS 流中留下可识别的痕迹。深度包检测，可以嗅探出客户端和服务器之间的联系消息，用以识别 TLS 版本，网络数据本身就可鉴别 TLS 流是否属于主流恶意软件家族。甚至在不同恶意软件家族使用同样的 TLS 参数的情况下，也能“基于流的特征”被鉴别出来。特征包括：流元数据[21]、包长度和时间的序列、字节分布、TLS 头信息。针对流分析的正确机器学习应用，可让这些特征在单独加密流的恶意软件归属问题上拥有可观的准确率。

4.3.3 技术：数据访问治理

■ 基本概念

数据访问治理包括政策、流程、协议和监督等方面职能，是指对数据存储单位中的数据分级分类访问权限进行实时跟踪、合规审核与风险评估的治理过程。

■ 主要实现

通常是针对存储在数据库中的数据，采用实时检测、用户访问行为分析、业务风险评估、动态风险评估、安全影响评估、优化管理等措施来保障数据安全治理整体工作的有效开展。

4.3.3.1 扩展技术：UEBA 用户实体行为分析

[21] 流元数据，是指输入输出的字节、包、网络端口号、流持续时间等。

■ 基本概念

UEBA 用户实体行为分析，是指提供画像及基于各种分析方法的异常检测，通常是基本分析方法（利用签名的规则、模式匹配、简单统计、阈值等）和高级分析方法（监督和无监督的机器学习等）用打包分析来评估用户和其他实体（主机、应用程序、网络、数据库等），发现与用户或实体标准画像或行为相异常的活动所相关的潜在事件。这些活动包括受信内部或第三方人员对系统的异常访问（用户异常），或外部攻击者绕过安全控制措施的入侵（异常用户）。

UEBA 可以识别历来无法基于日志或网络的解决方案识别的异常，是对安全信息与事件管理（SIEM）的有效补充。它是一个完整的系统，涉及到算法、工程等检测部分，以及用户实体风险评分排序、调查等用户交互、反馈。

图 9 典型的 UEBA 系统架构

■ 主要实现

从架构上来看，UEBA 系统包含三个层次，分别是数据中心层、算法分析层、场景应用层。其中，算法分析层一般运行在实时流处理、近线增量处理、离线批量处理的大数据计算平台之上。该平台运行着传统的规则引擎、关联引擎，同时

也支持人工智能引擎，如基线及群组分析、异常检测、集成学习风险评分、安全知识图谱、强化学习等 UEBA 核心技术。

4.3.3.2 扩展技术：业务风控[54][55]

■ 基本概念

业务安全风控[42]服务可基于业务场景，结合 IP 画像、设备指纹、黑卡检测、威胁情报等多维度信息实时进行风险识别，通过 API 接入，获取业务中 IP、号码、APP、URL 等画像数据，对其风险进行精确评估，做到对业务风险、黑产攻击实时感知、评估、应对、止损。

■ 主要实现

选择调用 sdk 服务获取设备指纹信息，再调用活动防刷接口，具体字段参考接口文档。以 API 形式输入字段后，经过活动防刷规则引擎，复合风控模型，威胁情报等技术能力的校验,提高识别的准确率。以风险等级风险标签的形式输出，可根据风险等级配置不同的处理策略，且通过风险标签获得原因。

4.3.3.3 扩展技术：动态风险评估

■ 基本概念

动态风险评估[56][57][58][59]，是指通过实时网络数据的监测、分析，进行网络风险的实时预报和评估。它是基于网络检测报警和攻击行为信息的网络安全动态实时风险评估模型，该模型充分利用 Petri 网和蒙古逻辑的优点，对已知和未知的攻击能够及时的检测和预报，并且能够很好的定量和定性网络攻击的风险，简单方便和有效的网络安全风险分析和屏幕过程，

■ 主要实现

采用模糊逻辑和Petri 网方法（FLPN）对待风险评估是作为一个动态实时推理过程，而不是静态统计过滤问题。FLPN 方法能够描述被入侵检测，报警观察和攻击传递行为完成的不同攻击步骤之间的关系。且用概率（或置信度）关联每一个工具状态。这种方法可以在短时间内定位风机预报攻击的后续行为，发现潜在的网络安全风险和提供可信的风险评估。

4.3.3.4 扩展技术：安全影响评估

■ 基本概念

数据安全影响评估[57][58][59]，是指依据有关信息安全标准，对信息系统及由其处理、传输和存储的数据信息的保密性、完整性和可用性等安全属性进行科学评价的过程。它要评估系统数据所面临的威胁以及脆弱性被威胁源利用后安全事件发生的可能性，并结合资产的重要程度来识别信息系统的安全风险等级。

■ 主要实现

数据安全影响评估主要有自评估和委托评估两种形式。自评估是指信息系统拥有、运营或使用单位发起的对本单位信息系统进行的风险评估。委托评估是指委托具有相应专业资质的第三方机构提供技术支持。由于数据安全影响评估的敏感性，涉及关键资产和核心信息部分，参与评估工作的人员均应遵守国家有关保密法规，对涉及的保密事项，应采取相应措施，签订保密协议并承担相应责任。数据安全影响评估作为信息安全保障工作的基础性工作和重要环节，应贯穿于信息系统及数据使用全生命周期。

4.3.4 技术：安全审计

■ 基本概念

安全审计，主要是指通过检测组织针对数据平台的日常服务和运维是否开展安全审计，并验证安全审计是否具有自动分析和报警功能的行为。

■ 主要实现

安全审计主要内容分为两项：一是检查是否对数据平台部署独立、实时的审计系统；二是验证数据平台的安全审计系统是否具有日志自动分析功能。主要包括主机安全审计、网络安全审计、数据库安全审计、业务安全审计和数据流转审计等环节。

4.3.4.1 扩展技术：主机安全审计[60]

■ 基本概念

主机安全审计，是指组织为确保主机及其存储信息的安全，对单台主机的安全审计。这是最基础的审计也是最复杂的审计，采取包括主机访问控制、用户身份鉴别、入侵及恶意代码防范等保护措施以及主机资源监控和安全审计等手段，确保主机资源的可用性并实现对主机重要操作等用户行为的安全监控和审计，同时满足对日志管理的合规要求。

■ 主要实现

通过在服务器、用户电脑或其他审计对象中安装客户端的方式来进行审计，可达到审计安全漏洞、审计合法和非法或入侵操作、监控上网行为和内容以及向外拷贝文件行为、监控用户非工作行为等目的。包括了主机日志审计、主机漏洞

扫描产品、主机防火墙和主机 IDS/IPS 的安全审计功能、主机上网和上机行为监控等类型的产品。

4.3.4.2 扩展技术：网络安全审计

■ 基本概念

网络安全审计[61][62][63]，是指在一个特定的网络环境下，为了保障网络和数据不受来自外网和内网用户的入侵和破坏,而运用各种技术手段实时收集和监控网络环境中每一个组成部分的系统状态、安全事件，以便集中报警、分析、处理的一种技术手段。

■ 主要实现

通过旁路和串接的方式实现对网络数据包的捕获，而且进行协议分析和还原，可达到审计服务器、用户电脑、数据库、应用系统的审计安全漏洞、合法和非法或入侵操作、监控上网行为和内容、监控用户非工作行为等目的。根据该定义，事实上网络审计已经包括了网络漏洞扫描产品、防火墙和 IDS/IPS 中的安全审计功能、互联网行为监控等类型的产品。

4.3.4.3 扩展技术：数据库安全审计

■ 基本概念

数据库安全审计，是指通过对用户访问数据库行为的记录、分析和汇报，来帮助用户事后生成合规报告、事故追根溯源；同时通过大数据搜索技术提供高效查询审计报告，定位事件原因，以便日后查询、分析、过滤，实现加强内外部数据库网络行为的监控与审计，提高数据资产安全的行为。

■ 主要实现

利用数据分类分级管理成果建立成熟有效的更新机制，对访问敏感的数据库表、字段进行重点审计。基于AI能力的数据基线，从用户帐号、获取敏感数据量、执行时间段、流量等用于综合判断异常。采用旁路部署的方式，通过镜像或探针的方式采集所有数据库的访问流量，并基于SQL语法、语义的解析技术，记录下数据库的所有访问和操作行为。

4.3.4.4 扩展技术：业务安全审计

■ 基本概念

业务安全审计[64][65]，是指对业务系统交互状态和企业信息化相关的参与者（研发人员、软件外包公司、运维人员、审计人员和普通用户等所有能接触到业务系统的相关人员）进行业务操作行为审计的行为。全过程包括业务系统与用户交互信息收集、异常行为告警、敏感信息深度检测、实时告警及违规行为回溯等环节。

■ 主要实现

采用了机器学习技术、网络流量分析技术、业务关联审计技术、大数据技术实现对业务违规操作行为的预警，对非法操作事件追踪、定位，有效防范业务系统的敏感数据被合法人员非法使用。对业务违规行为、信息安全隐患进行全面细致的监测审计，并能够为违规事件提供实时告警和事后溯源。

4.3.4.5 扩展技术：数据流转审计

■ 基本概念

数据流转审计，是指为了保证数据在收集，合并和展示等阶段链路的高可信赖性，针对数据生命周期中的收集存储、流式计算、OLAP 查询等环节进行审计的行为。

■ 主要实现

对流转过程中数据的识别和监测，可以帮助数据管理者在掌握网络流量中的重要敏感数据、业务系统、接口、数据库服务等的分布情况之后，有针对性地实施配套安全监管部署，提升整体安全防护能力。

 # 异常访问监测

访问控制管理，是指组织为防止信息资源遭受未经授权的访问，确保其在合法的范围内使用，所采取的物理和逻辑的控制手段，并借助有效的用户身份识别和访问控制策略，对身份和权限进行管理，特别当组织存在用户远程接入时，重点对其进行安全管理。该项的审计目的旨在通过对组织物理访问控制、逻辑访问控制以及账号权限的检查，判断组织是否对组织及信息系统所处区域实施物理安全防护，避免未授权的访问、损坏或干扰，以及是否根据组织既有的访问控制策略，针对单个用户或组用户对组织资源的访问控制规则和权力进行逻辑控制；此外，通过对远程接入管理的检查，检查远程工作活动是否安全、受控，从而确保远程工作场地的安全，防止设备和信息被盗、未授权泄露信息、远程访问滥用。

 # 安全事件分析

安全事件分析管理，是指组织以安全管理中心的形式，将制度流程、技术工具和人员统一集中管理应对日常网络安全事件，并通过建立具备安全态势感

知和预警的能力，对网络安全事件采取积极、主动的防御措施。通过检查组织对信息安全体系运行进行集中管理，以及对安全事件、恶意代码、安全日志、安全知识等安全相关事项进行集中管理的力度，决定是否优化安全事件、安全监控、访问控制、防恶意代码、安全审计等方面的日常安全工作。

4.3.5 技术：共享监控

■ 基本概念

共享监控[66][67]，是一种基于应用特征的终端识别方法，是指针对在业务系统之间流转或对外提供服务过程中 API 接口调用未授权或调用异常的监测。

■ 主要实现

在数据共享过程中，需要采取相应的共享安全监控措施实时掌握数据共享后的完整性、保密性和可用性。基于 HTTP 报文 User-agent 字段识别网络接入终端，可对网络中用户私接设备共享上网的行为进行识别和控制；通过针对共享数据的监测管控，防止数据丢失、篡改、假冒和泄漏。

4.3.5.1 扩展技术：风险操作监测

■ 基本概念

风险操作监测，是指主要针对包括内部人员、运维人员、业务开发合作厂商等人员操作核心业务系统异常操作的监测行为。包括利用通用的已知审计监测模型，以及利用大数据机器学习模型，建立行为基线 AI 分析行为的能力。

■ 主要实现

AI 分析主要是在行为基线异常波动特征监测上，考虑时间序列、调用内容分布等多维特征，充分混洗用户访问数据及接口调用数据，利用 DTM（动态主题模型）进行标签训练，同时引入 LSTM 神经网络训练异常识别模型，通过容器封装实现模型的敏捷生产应用，快速提升发现效果。从数据泄露类、账号权限类、操作违规类、流程违规类四个方面发现异常操作和未知的风险。

4.3.5.2 扩展技术：交换策略监测

- 基本概念

交换策略监测，是指针对于数据信息的发送和接收需建立安全、可控、便捷的跨网数据交换通道及策略，实现事前可控、事中可查、事后可溯的跨网数据交换全生命周期策略监测管控的行为。

- 主要实现

追溯数据交换操作行为和内容、指定人员的文件访问下载记录、文件审批行为记录。传输过程全加密，确保交换过程数据完整与安全。分布式部署架构，采用私有通信协议，抵御外部攻击能力强，审批通过前数据物理位置不跨网。重要文件审批才能发送满足各类审批要求，保护知识产权不流失。

4.3.5.3 扩展技术：接口访问预警

- 基本概念

接口访问预警，是指在业务系统之间流转或对外提供服务过程中对接口调用未授权或调用异常的检测预警。

- 主要实现

对于平台与平台之间的接口，需要使用一些身份认证机制，比如：APPID 或 APPKey 和 APPSecret、token。对于前后端接口调用的情况，不要全部按前端传入的次数进行处理，要由后端做二次校验，严格对权限进行控制；后端需要自动二次获取用户的相关权限信息。以此减少验证权限环节存在的缺陷。

4.4 R:响应

R：响应是 D：检测的极其重要的后手动作，是 DR 模型的重要一环。本文收录了事件发现，事件处置，应急响应，事件溯源等四个技术。

4.4.1 技术：事件发现

■ 基本概念

安全事件发现是数据安全事件响应的第一步，是指通过主动发现和被动发现，确认入侵检测机制或另外可信站点警告已入侵，以及主动监测数据可能泄露的点，第一时间定位和处理，是实行紧急预案。

■ 主要实现

安全事件发现的主要实现方式为通过对信息网络系统进行初始化快照、采用应急响应工具包等。

 # 系统快照

常规情况下，信息系统进程、账号、服务端口和关键文件签名等状态信息的记录。通过在系统初始化或发生重要状态改变后，在确保系统未被入侵的前提下，立即制作并保存系统快照，并在检测的时候将保存的快照与信息系统

当前状态进行对比，是后续“检测”安全事件的一种重要途径。同时，通过态势感知、Net- Flow 技术等技术辅助发现。

4.4.2 技术：事件处置

■ 基本概念

事件处理[72]是指安全事件发生之后，采取常规的技术手段处理应急事件，目前包括了事件还原和流量分析等技术，一方面分析安全事件发生的原因，一方面减小安全事件造成的影响或者损失。法律法规方面，《中华人民共和国数据安全法》对于有关部门在发生数据安全事件时的处理作了相关说明：“发生数据安全事件，有关主管部门应当依法启动应急预案，采取相应的应急处置措施，防止危害扩大，消除安全隐患，并及时向社会发布与公众有关的警示信息。”，同时对相关数据处理的主体也做了责任说明：“发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。”

■ 主要实现

事件处理的主要实现方式为及时抑制。抑制是指对攻击所影响的范围、程度进行扼制，通过采取各种方法，控制、阻断、转移安全攻击。抑制阶段主要是针对前面检测阶段发现的攻击特征，比如攻击利用的端口、服务、攻击源、攻击利用系统漏洞等，采取有针对性的安全补救工作，以防止攻击进一步加深和扩大。抑制阶段的风险是可能对正常业务造成影响，如系统中了蠕虫病毒后要拔掉网线，遭到 DDoS 攻击时会在网络设备上做一些安全配置，由于简单口令遭到入侵后要更改口令会对系统的业务造成中断或延迟，所以在采取抑制措施时，必须充分考虑其风险。

4.4.3 技术：应急响应

■ 基本概念

“应急响应”[68][69][70][71]对应的英文是“Incident Response”或“Emergency Response”等，通常是指一个组织为了应对各种意外事件的发生所做的准备以及在事件发生后所采取的措施。

■ 主要实现

应急响应的主要实现方式为准备（预防：扫描、风险分析、打补丁）、检测（事件是否发生，事件产生的原因和性质）、遏制（隔离网络、修改防火墙或者路由器规则、删除攻击者登录账号、关闭被利用的服务器或者主机）、根除（分析原因、进行安全加固）、恢复（恢复系统备份）跟踪（关注效果）等。

4.4.4 技术：事件溯源

■ 基本概念

安全事件溯源，是指根据入侵者的入侵痕迹进行全方位的追踪和分析，也是应急响应的重要一环。比如可以采用高置信度行文审计，定责的数据访问审计可以记录识别到的主客体信息，在记录操作行为的同时，能够对每条审计日志进行签名，不仅做到独立于应用系统的第三方审计，还能够通过数字签名技术确保审计日志的不可篡改，以及在事后追溯问题过程中提供重要依据。

■ 主要实现

安全事件溯源的主要实现方式为攻击源捕获、溯源反制等。

 # 攻击源捕获

攻击源捕获的技术实现包括：安全设备报警，如扫描 IP、威胁阻断、病毒木马、入侵事件等；日志与流量分析，异常的通讯流量、攻击源与攻击目标等；服务器资源异常，异常的文件、账号、进程、端口，启动项、计划任务和服务；邮件钓鱼，获取恶意文件样本、钓鱼网站 URL 等；蜜罐系统，获取攻击者行为、意图的相关信息。

 # 溯源定位手段

溯源反制手段的技术实现包括：IP 定位技术：根据 IP 定位物理地址—代理 IP；ID 追踪术：搜索引擎、社交平台、技术论坛、社工库匹配；网站 url：域名 Whois 查询—注册人姓名、地址、电话和邮箱；恶意样本：提取样本特征、用户名、ID、邮箱、C2 服务器等信息—同源分析；社交账号：基于 JSONP 跨域，获取攻击者的主机信息、浏览器信息、真实 IP 及社交信息等。[73]

4.5 R:恢复

恢复是安全事件发生后，主要补救手段，通常会涉及网络恢复、设备恢复、业务恢复、数据恢复等，基于本文主旨，特别强调数据恢复。

4.5.1 技术：灾难恢复

- 基本概念

灾难恢复，是指自然或人为灾害后，重新启用信息系统的数据、硬件及软件设备，并恢复正常商业运营的过程。

- 主要实现

其核心是对企业或机构的灾难性风险作出评估、防范，特别是对关键性业务数据、流程，给予记录、备份及保护，尽可能迅速地将平台恢复到正常运营的状态。

4.5.1.1 扩展技术：数据备份

- 基本概念

数据备份，是指为防止系统出现操作失误或系统故障而导致数据丢失，将全部或部分数据集合从当下存储单位复制到其它存储介质的过程。

- 主要实现

传统的数据备份主要是采用内置或外置的磁带机进行冷备份，目前随着技术不断发展，不少企业开始采用网络备份，网络备份一般都是通过专业的数据存储管理软件结合相应的硬件和存储设备来实现。

 # 集群技术[74][75][76]

由两台或多台节点机（服务器）构成的一种松散耦合的计算节点集合，为用户提供网络服务或应用程序(包括数据库、Web 服务和文件服务等)的单一客户视图，同时提供接近容错级的故障恢复能力。集群系统一般通过两台或多台节点服务器系统通过相应的硬件及软件互连，每个群集节点都是运行其自己进程的独立服务器。这些进程可以彼此通信，对网络客户机来说就像是形成了一个单一系统，协同起来向用户提供应用程序、系统资源和数据。除了作为单一系统提供服务，集群系统还具有恢复服务器级故障的能力。

4.5.1.2 扩展技术：容侵技术

■ 基本概念

容侵、即容忍入侵技术，是指系统在入侵已发生的情况下，能保证关键功能继续执行，关键系统能够持续的提供服务。

■ 主要实现

常见的容侵技术手段有冗余、多样化、门限密码、群组通信、表决、代理、封装等。

4.5.1.3 扩展技术：容错技术

■ 基本概念

容错技术，是指当由于种种原因在系统中出现了数据、文件损坏或丢失时，系统能够自动将这些损坏或丢失的文件和数据恢复到发生事故以前的状态,使系统能够连续正常运行的一类技术。

■ 主要实现

容错技术是容忍并防范局部错误的决策方法,是提高决策可靠性的重要方法之一。容错技术目前包括双重文件分配表和目录表技术、快速磁盘检修技术、磁盘镜像技术、双工磁盘技术等。

4.5.1.4 扩展技术：容灾技术

■ 基本概念

容灾技术[77]，即灾难发生时，在保证生产系统数据尽量少丢的情况下，保证系统业务的不间断运行。容灾技术是信息系统的高可用技术的一个组成部分，按

照容灾距离划分，容灾技术分为本地容灾和异地容灾；按照保护级别划分，容灾技术可分为数据级别容灾、应用级容灾和业务级别容灾。

1）按照容灾距离

本地容灾：一般指主机集群，当某台主机发生故障，其它主机可以代替该主机，继续正常对外提供服务。

异地容灾:是指在与生产机房一定距离的异地建立与生产机房类似的备份中心，并采用特定的技术将生产中心的数据传输到备份中心。

2）按照保护级别

数据级容灾：这属于最基础的手段，指通过建立异地容灾中心，进行数据的远程备份，发生灾难时应用会中断。

■ 主要实现

应用级容灾：主要针对关键应用进行的容灾方案，应用级容灾是建立在数据级容灾基础上，对应用系统进行实时复制，即在备份站点构建一套相同的应用系统，通过同步或异步复制技术，保障关键应用在允许的时间范围内恢复运行。

业务级容灾：是最高级别的容灾手段，它包括除了保障 IT 系统业务连续性外也提供非 IT 系统保障，业务级容灾是在数据级容灾和应用级容灾基础之上，还需要考虑 IT 系统之外的业务因素。

 # 云灾备[78][79]

指灾备业务的云端实现形式，主要包括云备份与云容灾。其中云备份是指备份技术将生产存储数据直接备份到云端，进而实现数据备份与恢复功能；云

容灾则是指通过数据、系统的云端迁移、高可用等方式实现业务的快速接管，保证业务连续性。与传统的用户在本地或异地灾备模式不一样。云灾备是一种为了适应云和大数据时代下的服务模式，将文件、数据卷、数据库、操作系统、虚拟机等灾备到云端。在具体的实际场景应用中，云灾备包括了传统的数据存储和定时复制，以及新一代的数据实时复制、CDP 保护、系统热迁移、应用切换和 CDM 管理，涉及到存储双活、云端备份、云端多活容灾等。云灾备服务独有的高性能、高可靠性、高扩展性、易维护性、责任风险低以及高性价比的服务特色，采用当前最先进、安全、可靠的数据备份和数据复制技术，建设可管理、可运营的灾备服务，以保证在灾难发生后能够快速、准确的恢复业务数据和关键应用系统，保障客户业务的连续运行。

4.5.2 技术：数据迁移技术（分层存储管理）

■ 基本概念

数据迁移[80][81]是一种将离线存储与在线存储融合的技术，是将很少使用或不用的文件移到辅助存储系统的存档过程。这些文件通常是需在未来任何时间可进行方便访问的图像文档或历史信息。迁移工作与备份策略相结合，并且仍要求定期备份。

■ 主要实现

数据迁移的实现可以分为 3 个阶段：数据迁移前的准备、数据迁移的实施和数据迁移后的校验。充分周到的准备是完成数据迁移工作的主要基础，具体是要进行待迁移数据源的详细说明(包括数据的存储方式、数据量、数据的时间跨度)；建立新旧系统数据库的数据字典；对旧系统的历史数据进行质量分析，新旧系统

数据结构的差异分析；新旧系统代码数据的差异分析；建立新老系统数据库表的映射关系，对无法映射字段的处理方法；开发、部署 ETL 工具，编写数据转换的测试计划和校验程序；制定数据转换的应急措施等。

4.5.3 技术：本地双机热备

双机热备应对服务器的故障最可靠最高效的灾难恢复技术，可能有效降低设备故障、操作系统故障、软件系统故障引起的数据丢失或业务宕机。

■ 基本概念

双机热备特指基于 active/standby 方式的服务器热备。服务器数据包括数据库数据同时往两台或多台服务器执行写操作，或者使用一个共享的存储设备。

■ 主要实现

共享方式和软同步数据是双机热备两种主流实现方式。

 # 共享方式

即两台服务器连接一个共享使用的存储设备或存储网络，通过安装双机软件实现双机热备。

 # 软同步数据

即利用纯软件方式或软件同步数据方式，两台服务器所需要的应用数据放在各自的服务器中，不使用共同的存储设备。

4.5.4 技术：远程异地容灾

■ 基本概念

远程容灾系统一般由生产系统（即数据中心）、可接替运行的备份中心、数据复制系统、通信线路等部分组成。在正常生产和数据备份状态下，生产系统向备份系统传送需备份的数据。灾难发生后，当系统处于灾难恢复状态时，备份系统将接替生产系统继续运行。

■ 主要实现

远程异地容灾技术要求容灾系统满足基本建设要求：

1) 备份中心与数据中心在距离上要足够远，使得当数据中心遭受灾害破坏时，不会影响到备份中心；
2) 必须保证备份中心与数据中心的数据同步；
3) 备份中心的所有应用系统必须经过严格的测试，确保业务系统能够正常运行；
4) 备份中心与数据中心间为保持数据同步而需传输的数据量，以及两地间的网络带宽，以及网络带宽必须能够保证两地间数据的顺畅同步；
5) 备份中心的计算机系统有足够的处理能力来接管数据中心的业务；
6) 数据中心与备份中心的应用切换快速可靠，并可进行自动和手工切换。

4.6 C:反制

数据被侵害或被侵权很难根本杜绝。那么，有必要考虑或假想确定遭受数据攻击，数据泄露后，如何积极应对，同时考虑实施积极的反制技术威慑和震慑敌手。故，本文 DTTACK 模型特别强调了反制的重要性。考虑商业实用性，本版本收录水印技术、溯源技术、版权管理技术等内容。

4.6.1 技术：水印技术

■ 基本概念

数字水印技术是一种将特制的、不可见的标记，利用数字内嵌的方法隐藏在数字图像、声音视频等数字内容中，由此来确定版权拥有者、认证数字内容来源的真实性、识别购买者、提供关于数字内容的其他附加信息、确认所有权认证和跟踪侵权行为的技术。[83]

■ 主要实现

水印技术包括图像水印、媒体水印、数据库水印、屏幕水印等。

4.6.1.1 扩展技术：图像水印

■ 基本概念

图像水印使用不可察觉的方式修改图像后、嵌入图像,用于版权保护等用途。

■ 主要实现

根据水印的实现过程，图像水印算法可分为空域算法和变换域算法。

空域算法是通过直接改变原始图像的像素值来嵌入水印,通常具有较快的速度，但鲁棒性差，且水印容量也会受到限制;

变换域算法是通过改变某些变换系数来嵌入水印,通常具有很好的鲁棒性和不可见性。其实现一般是基于图像变换，如 DCT、DFT、DWT 等。

4.6.1.2 扩展技术：多媒体水印

■ 基本概念

多媒体水印，代表数字控制和数字媒体的汇合，多媒体技术是一种把文本、图形、图像、动画和声音等多种信息类型综合在一起，并通过计算机进行综合处理和控制，能支持完成一系列交 互式操作的信息技术。

■ 主要实现

媒体水印是通过对媒体文件的冗余特点来嵌入水印，既不影响媒体质量，又能达到保护媒体版权和控制产品复制的目的。

4.6.1.3 扩展技术：数据库水印

■ 基本概念

数据库水印是指通过数据库中的数据进行修改、标记，将特定的数字信号嵌入数字产品中，以起到数据所有权判定与数据完整性验证的作用。

■ 主要实现

从原始环境向目标环境进行敏感数据交换时,通过一定的方法向数据中植入水印标记，从而使数据具有可识别分发者、分发对象、分发时间、分发目的等因素，同时保留目标环境业务所需的数据特性或内容的数据处理过程。

4.6.1.4 扩展技术：屏幕水印

■ 基本概念

屏幕水印技术以桌面水印的形式在内网终端计算机桌面上显示，可通过文本、点阵、二维码等不同形式将使用终端相关信息投射到终端计算机桌面上。该屏幕水印可在应用系统页面、桌面、网页、办公文档、远程桌面等各种场景下显示。

■ 主要实现

主要通过文本水印、点阵水印、二维码水印等技术实现。

4.6.2 技术：溯源技术

数据溯源指记录原始数据在整个生命周期内(从产生、传播到消亡)的演变信息和演变处理内容，进而可以根据追踪路径重现数据的历史状态和演变过程，实现数据历史档案的追溯。

■ 基本概念

数据溯源指对目标数据的源头数据以及流转过程中的变动加以追溯、确认、描述和记录保存的过程[84]，其主要包含三部分内容：

1) 对产生当前数据项的源头数据的追溯与描述；

2) 对源头数据如何演变为当前数据状态的过程信息的追溯、捕获或记录；

3) 对所有能够影响数据状态的因素(比如影响数据的实体、工具等)进行追溯、描述和记录。

■ 主要实现

一般情况中，数据溯源技术通过构建数据溯源模型，利用附加信息或计算等数据溯源追踪方法，实现对数据可靠性确认。

结合场景，数据溯源模型[22]主要包含：流溯源信息模型、时间-值中心溯源模型、四维溯源模型、开放的数据溯源模型、Provenir 数据溯源模型、数据溯源安全模型、PrInt 数据溯源模型等。

[22] GB/T34945-2017《信息技术数据溯源描述模型》定义了 ProVOC(Provenance Vocabulary Model)数据溯源模型，该模型由数据、活动和执行实体 3 个一级类构件组成。“数据”包括“参数”和“数据集”两个二级子类构件。

常用的数据溯源追踪方法主要包含：标注法、反向查询法、通用的数据追踪方法、双向指针追踪法、图论追踪法以及专用查询语言追踪法等。

在数据安全保护场景中实现数据溯源技术,还可以利用其它工程实践中较成熟的技术，比如权限流转、权限迁移和签名验证等。

4.6.2.1 扩展技术：权限流转

- 基本概念

在对数据源头溯源、数据拥有者身份溯源以及确保溯源数据可信情况下，可以利用权限流转技术，如区块链，让对数据处理的权限在每一个环节进行流转。

- 主要实现

利用物联网技术、RFID 等技术，在商品数据流转过程中，把全过程流转数据和权限数据写入区块链。确保区块链上信息不能随意篡改和只接受授权修改，解决数据溯源和溯源信息真实性。

4.6.2.2 扩展技术：权限迁移

- 基本概念

权限迁移指把用户对原始数据集操作权限与新数据的操作权限进行一一影射。通常会在数据迁移过程中，同步实现操作人权限迁移。

- 主要实现

较常见的权限迁移包含数据库操作权限迁移，域控制器下权限迁移，以及利用专用协议（利用临时权限绑定原始权限，在原始权限迁移到新数据集时，再完成解绑）。

4.6.2.3 扩展技术：签名验证

■ 基本概念

本处签名验证技术指对数据集合利用多次签名，实现对面数据拥有者身份溯源和数据完整性溯源管理。

■ 主要实现

利用加密算法或加密协议或加密软件，对结合数据处理者身份信息对数据集进行多次签名。在需要对数据进行溯源时，对数据集进行多次验证，以确认签名者身份。

4.6.3 技术：版权管理技术

版权管理技术放置于DTTACK模型最后一个技术模块旨在强调：从技术角度考量，版权管理是最后的手段。在数据安全工作中，数字版权破坏和数字版权不正当使用后,如果有版权管理技术支撑,对于组织后续维权和追责具有重大意义。

■ 基本概念

本文的版权管理技术特指数字版权管理（Digital Right Management，DRM），即密码技术、去标识化技术、水印技术从技术上防止对数字内容的非法复制和非法使用。

■ 主要实现

数字版权管理提供了对数字内容进行安全分发、权限控制和运营管理的能力，使得数字内容相关权益方能对每个数字内容定义不同的使用权限、每个权限

对应不同的商业价值和价格。相关用户只有得到授权后才能按照相应的权限消费数字内容。数字版权管理常见实现手段包含：

 # 加密技术

对数字化作品进行加密，使得已实施版权保护的数字作品或商品，只有通过解密的逆变换，方可阅读或其他方式进行使用。

 # 数字证书技术

对数字作品或商品进行数字证书签发，表明拥有证书的合法用户身份。证书通常包括证书申请者的名称和信息、申请者的公钥、证书颁发者 CA 的数字签名和一组控制信息。

 # 数字对象唯一标识符，（Digital Object Unique Identifier，DOI）

利用识别号解析协议对数字对象进行唯一标识符命名，使得数字产品或商品具备一个持久可追溯的鉴别特征。

 # 数字水印技术

将不妨碍对数据的正常使用特征信息，但它可嵌入到数字产品或商品，以实现对版权的跟踪和保护。

 # 安全容器技术

采用加密技术把数据包（拥有者特征，使用规则）封装在数字产品或商品中。

 # 移动代理技术

采用执行用户操作和程序功能的代码或程序，在特定节点或触发条件下，进行自我复制和子移动代理生成。

4.7 G:治理

DTTACK 模型本身不包含治理，但基于现实中，大量的数据安全本身基于合规监管，组织使命，企业文化而被推动。同时，在数据安全大命题下，积极的、科学的、人文的数据安全治理是极其重要的手段。故，本文把战术：治理作为模型扩展或补充。

4.7.1 数据价值

- 基本概念

结合马克思劳动价值理论，数据价值为数据交换价值[23]。数据总价值量为数据价值总量等于单位数据价值[24]乘以数据总数量。

本文给出另外一个模糊性概念以供参考：数据价值指数据在宏观经济、市场机制以及其它社会利益和个人利益中表现出的经济特征。

- 主要实现

在国内，数据价值还处于研究探索阶段。目前已有少量研究成果[85][91]，但更多主要集中在具体场景下微点突破，比如用数据证券化思路或特征业务场景进行数据价值评估[87-91]；再比如，利用增强算法估算数据价值[86]。

[23]根据实际经验，数据难以像传统商品做货币或物品交换，更多是共享行为

[24]单位数据价值很难估算，比如一个用户历史消费行为特征数据价值几何？同时，单位数据价值可能会引入是否支付个人数据费用的问题。

较早期或较成熟的实现思路是信息经济学、信息估值经典方法和数据资产估值，对数据资产做较精确评价。

4.7.1.1 信息经济学

■ 基本概念

宏观信息经济学又称情报经济学、信息工业经济学。以研究信息产业和信息经济为主，是研究信息这一特殊商品的价值生产、流通和利用以及经济效益的一门新兴学科。是在信息技术不断发展的基础上发展建立起来的，是经济学的重要领域[94]。

微观信息经济学又被称为理论信息经济学是从微观的角度入手，研究信息的成本和价格，并提出用不完全信息理论来修正传统的市场模型中信息完全和确知的假设。重点考察运用信息提高市场经济效率的种种机制。因为主要研究在非对称信息情况下，当事人之间如何制定合同、契约、及对当事人行为的规范问题，故又称契约理论或机制设计理论[94]。

较贴合数据资产概念的概念，由道格拉斯·B.莱尼（DouglasB.Laney）提出，确认信息资产持有者后，考量信息资产的量化及入账，用经济学原理处理数据[95]。

其中，信息估值是信息经济学中重要内容。

■ 主要实现

在国内，数据价值还处于研究探索阶段。目前已有少量研究成果[92][96]，提出数据估值模型，如图示《电子商务数据资产评价指标体系》[25]中的数据资产价值

[25]《电子商务数据资产评价指标体系》（GB/T37550-2019）适用于数据的电子商务交易过程中，对数据资产价值进行量化计算、评估评价，也可以作为在线数据交易过程中数据资产商品化、证券化的评价依据。

评价指标体系[96][97]，但更多主要集中在具体场景下微点突破，比如用数据证券化思路或特征业务场景进行数据价值评估[87-91]；再比如，利用增强算法估算数据价值[86]。

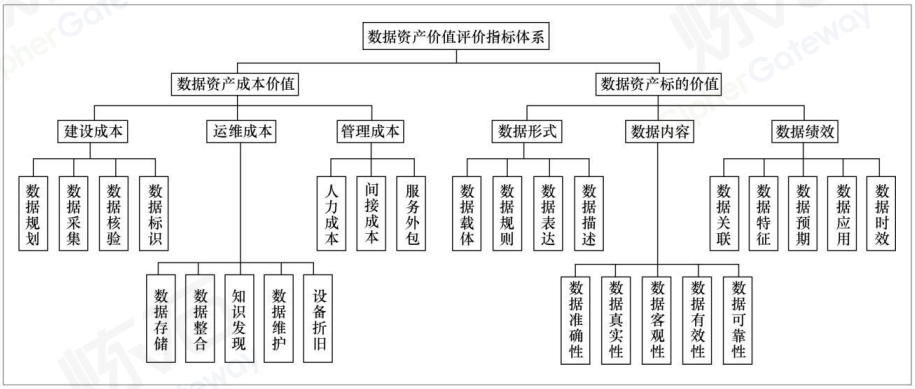

图 10 数据资产价值评价指标体系

道格拉斯·B.莱尼[95]提出使用信息资产的量化及入账，并用经济学原理处理数据。首先，做信息资产鉴定，如基本原则是：实体拥有和控制，可兑换为现金，且未来可产生和流入经济利益；其次，评估数据质量[26]；再次，建立评价模型（如图示所示：）；最后，引入信息内在价值（IVI）和商用价值(BVI)计算公式[27]。

图 11 Gartner 信息资产价值模型

[26]道格拉斯·B.莱尼引入有效性、完整性、一致性、独特性、精确性、及时性、可访问性、稀缺性、相关性、可用性、可信度、客观性等多个维度进行数据质量评估。

[27]道格拉斯·B.莱尼的模型可进行信息的经济价值（EVI）核算，鉴于文档字数据受限，详细实现请查阅道 Infonomics 原书内容。

IVI 计算公式：

$$有效性 \twoheadrightarrow 完整性 \twoheadrightarrow (1 - 稀缺性) \twoheadrightarrow 生命周期$$

BVI 计算公式：

$$\sum_{p=1}^{n} (关联度_p) \; 有效性 \twoheadrightarrow 完整性 \twoheadrightarrow 及时性$$ [28]

4.7.1.2 信息估值

■ 基本概念

信息公开或保密对于特定人物、特定时间、特定场景，所获得的收益、亏损、危险及其它影响[29]。

■ 主要实现

交易双方结合会计学和交易物的总体价值，并根据受偿意愿或支付意愿，完成信息估值。

4.7.1.3 数据资产价值管理

数字经济时代把组织或企业的数据作为基本生产要素之一，那么对于组织整个数据资源估值比信息估值更加有效、客观和合规[30]。

■ 基本概念

结合中国信息通信研究院发布的《数据价值化与数据要素市场发展报告（2021 年）》[97]提出数据价值化的“三化”框架，即数据资源化、数据资产化、数据资本化。组织或企业应当对资产化的数据资源进行数据资产价值管理。

[28] p 为业务流程和功能数量。
[29] 本处信息估值指类似情报信息价值评估。
[30] 本文讨论的数据资产特指国家法律法规许可下的可交易数据。

■ 主要实现

主要实现手段包含数据资产价值评估、数据资产定价。数据资产价值评估和数据资产定价是数据资产价值管理过程中不同阶段的独立行为。数据资产价值评估是对数据资产的使用价值进行度量，与数据资产是否被交易无关。在一定的时间周期内，数据资产的价值是固定的，因此数据资产价值评估是一个静态行为。数据资产价值评估在数据资产化阶段实现。数据资产的价格是动态变化的，因此数据资产定价是一个动态行为。数据资产定价在数据资产交易过程中实现[86]。

 # 数据资产价值评估

从数据资产不同价值维度，建立评价指标体系和指数，采用成本法、收益法、市场法、甚至 AI 算法、深度学习算法等评价的数据资产价值。

 # 数据资产定价

利用固定定价法、动态定价法、协商定价、拍卖定价、数据信息熵定价法，明确数据资产交易价格。

4.7.1.4 个人信息价值评估

■ 基本概念

评估个人信息市场价值[31][32]，进一步通过财务手段来控制个人信息的使用。

■ 主要实现

[31]金钱补偿可能是直接经济补偿，或是免费服务，抑或是其它无形得利形式。
[32]个人信息市场价值类似于个人信息货币化，来源于数据货币化，即（DataMonetization），利用数据获得可量化经济利益的过程。

在国内，数据价值还处于研究探索阶段。结合宏观经济，社会环境和公共利益，在遵循法律法规基础上，重点考虑个人信息的质量、敏感度、生命周期，实现市场化交易价值评估[33]。

4.7.2 数据安全策略

■ 基本概念

形式化或非形式化的描述组织总体安全规则的计划。

■ 主要实现

主要包含数据安全原则、数据安全隐私管理、法规行业安全要求等。

4.7.2.1 数据安全原则

■ 基本概念

开展数据安全工作时，组织或企业需要遵循的基本性原则，通常进行自顶向下的工作部署，进一步形成企业安全文化。

■ 主要实现

主要可分为纲领性原则和场景性原则。纲领性原则，如三同步管理原则，安全性原则，业务影响最小性原则；场景性原则，如数据分类分级时，就高不就低原则、关联叠加效应原则；如数据安全风险评估时，过程可控性原则、工具可控性原则等。

4.7.2.2 数据安全隐私管理

[33]现阶段个人信息价值评估有可能来自于受偿意愿、支付意愿，也有可能来自于数据泄露后接收方的法律成本。

《中华人民共和国个人数据保护法》、《中华人民共和国民法典》、《通用数据保护准则》（GDPR）、《2018 年加州消费者隐私法案》（CCPA）等，俱要加强个人隐私权和数据安全保护。组织或企业应急围绕解决隐私保护，建议战略性数据安全工程。

■ 基本概念

针对个人信息保护工作，利用行政管理、技术手段、法律文书、合同协议、意识教育等提升数据安全隐私管理水平。

■ 主要实现

结合《个人数据保护法》、GDPR、GB/T352732020《信息安全技术个人信息安全规范》等，常见的实现手段主要包含设计隐私主要包含设计隐私保护、默认隐私保护和隐私数据安全策略清单等。

 # 设计隐私保护

设计保护隐私（PrivacybyDesign，PBD)指通过设计保护隐私，最早由安卡沃基提出，是一种综合技术、运行系统、工作流程、管理结构、物理空间和基础设施的隐私设计理论。

在《通过设计的个人信息保护》一文中，学者郑志峰比较认可分为六大步骤的实施方案，即：(1)界定法律需求；(2)系统功能分析；(3)确定数据范围和类型；(4)隐私风险分析；(5)多边需求分析；(6)方案的实施和测试。

 # 设计和默认的数据保护

设计的数据保护是指在任何系统、服务、产品或流程的设计阶段以及全生命周期中充分考虑数据保护问题，从本质上来说，就是要将数据保护集成到数据处理活动和业务实践当中。

默认数据保护是指在默认情况下仅处理目的所需的个人数据，与目的限制原则及数据最小化原则息息相关。默认的数据保护要求在数据处理开始前确定所要处理的数据，以适当的方式充分告知数据主体并在整个处理过程中仅在目的范围内进行处理。

 # 隐私数据安全策略清单

隐私数据安全策略清单可以帮助企业管理数据安全、隐私保护安全策略和安全实现。结合 GB/T35273，个人信息保护政策发布个人信息保护政策是个人信息控制者遵循公开透明原则的重要体现，是保证个人信息主体知情权的重要手段，还是约束自身行为和配合监督管理的重要机制。个人信息保护政策应清晰、准确、完整地描述个人信息控制者的个人信息处理行为。

行业数据特别安全要求

 # 《工业和信息化领域数据安全管理办法（试行）》征求意见稿

为贯彻落实《数据安全法》等法律法规，加快推动工业和信息化领域数据安全管理工作制度化、规范化，提升工业、电信行业数据安全保护能力，防范数据安全风险，工业和信息化部研究起草了《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》。

 # 《人类遗传资源管理暂行办法》

第四条规定，国家对重要遗传家系和特定地区遗传资源实行申报登记制度；未经许可，任何单位和个人不得擅自采集、收集、买卖、出口、出境或以其他形式对外提供。

 # PCIDSS 安全策略

PCIDSS 对于所有涉及信用卡信息机构的安全方面做出标准的要求，其中包括安全管理、策略、过程、网络体系结构、软件设计的要求的列表等，全面保障交易安全。

PCI-DSS 安全认证的主要过程是由 VISA 和 MasterCard 授权的独立审查公司完成。是一次彻底对该支付公司在线支付系统的安全审查，其中有近 200 项审查内容。包含 6 大领域 12 项要求的规范，其认证过程异常严苛且繁杂，包括自我安全检测(Self Security Probe)、漏洞分析(Analysis of the Vulnerabilities)以及由协会执行的安全调查(Security Investigation by the Council)三个阶段，考察范围涉及硬件、软件、员工和公司管理等多项指标。

4.7.3 数据安全模型

■ 基本概念

安全模型的意义在于从不依赖于软件实现的，高层次上的概念模型且要反映一定的安全策略。

在网络安全领域，密码技术和访问控制技术具备可验证的安全模型，其它风险管理领域和网络防护领域的安全模型俱为工程意义上实践模型。安全模型可以指导安全工作，提高工作效率。

■ 主要实现

本文重要分析了 DSG 模型、CARTA 模型、DGPC 框架以及 FinDRA 模型。

4.7.3.1 DSG 框架

■ 基本概念

DSG 框架建议数据管理与信息安全管理两个小组团队，针对整合的业务数据生命周期过程进行业务影响分析(BIA)，发现的各种数据隐私和数据保护风险，以降低整体的业务风险。

1) 利用应用数据发现技术为每个数据集的容量、变化和准确性确定范围。

2) 识别每个数据集产生的业务风险和财务影响并确定优先顺序。

3) 检查影响每个数据集的数据存储涉及法律合规问题。

4) 应用数据分类和主数据策略来优先确定哪些数据集需要安全性。

5) 为每个数据集创建访问和使用策略，并确保这些策略在所有可用数字业务环境保持一致。

■ 主要实现

Gartner DSG 模型分五个步骤实现：

步骤一：业务需求与安全（风险/威胁/合规性）之间的平衡：这里需要考虑 5 个维度的平衡：经营策略、治理、合规、IT 策略和风险容忍度，这也是治理队伍开展工作前需要达成统一的 5 个要素。经营策略、治理、合规、IT 策略、风险容忍度

步骤二：数据优先级：进行数据分级分类，以此对不同级别数据实行合理的安全手段。

步骤三：制定策略，降低安全风险：从两个方向考虑如何实施数据安全治理，一是明确数据的访问者（应用用户/数据管理人员）、访问对象、访问行为；二是基于这些信息制定不同的、有针对性的数据安全策略。

步骤四：实行安全工具：数据是流动的，数据结构和形态会在整个生命周期中不断变化，需要采用多种安全工具支撑安全策略的实施。Gartner 在 DSG 体系中提出了实现安全和风险控制的 6 个工具：Crypto、DCAP、DLP、CASB、IAM、UEBA，这 6 个工具是指 6 个安全领域，其中可能包含多个具体的技术手段。

步骤五：策略配置同步：策略配置同步主要针对 DCAP 的实施而言，集中管理数据安全策略是 DCAP 的核心功能，而无论访问控制、脱敏、加密、令牌化，哪种手段都必须注意对数据访问和使用的安全策略保持同步下发，策略执行对象应包括关系型数据库、大数据类型、文档文件、云端数据等数据类型。

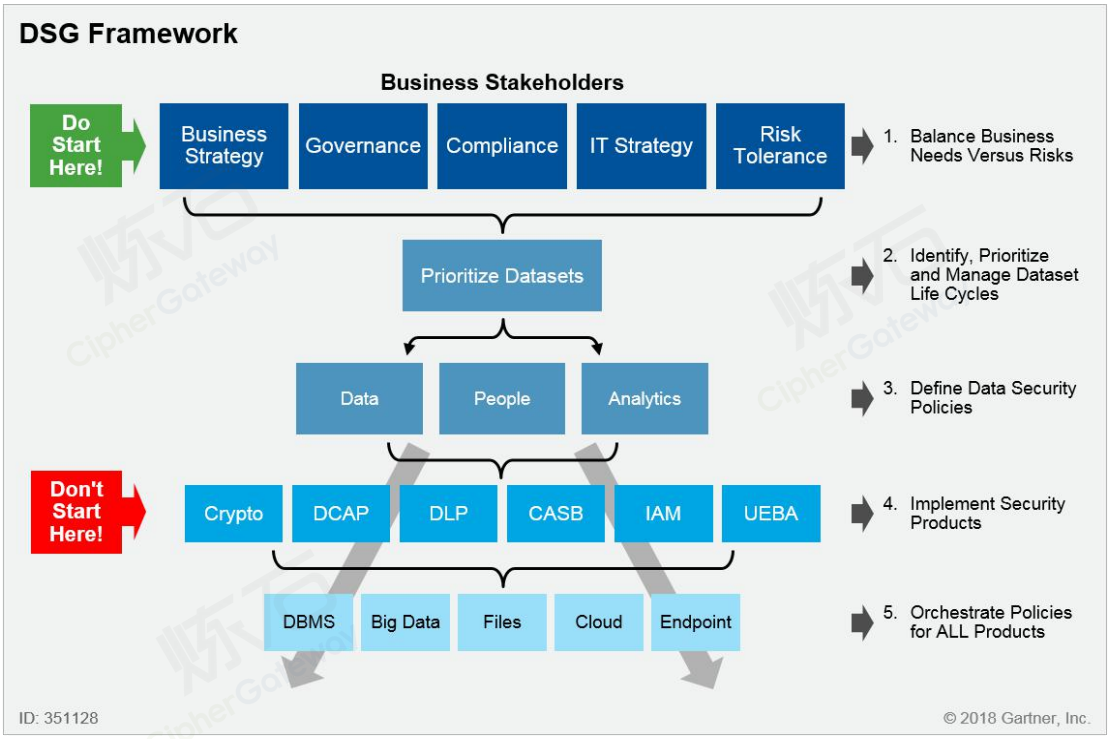

图 12 GartnerDSG 框架图

4.7.3.2 CARTA 模型

■ 基本概念

2017 年 Gartner 提出了持续自适应的安全风险和信任评估模型（CARTA），旨在使安全与风险管理的领导者在持续的和自适应的风险与信任评估的基础上，对于实时出现的各类事件做出及时和合理的反应，在风险可接受的程度上保障数字业务的健康运行。CARTA 的方法同样适用于数据安全评估与控制。CARTA 模型的核心——基于大数据分析与评价的动态安全决策。

■ 主要实现

CARTA 模型主要分为四个阶段，即预防、检测、预测、响应。

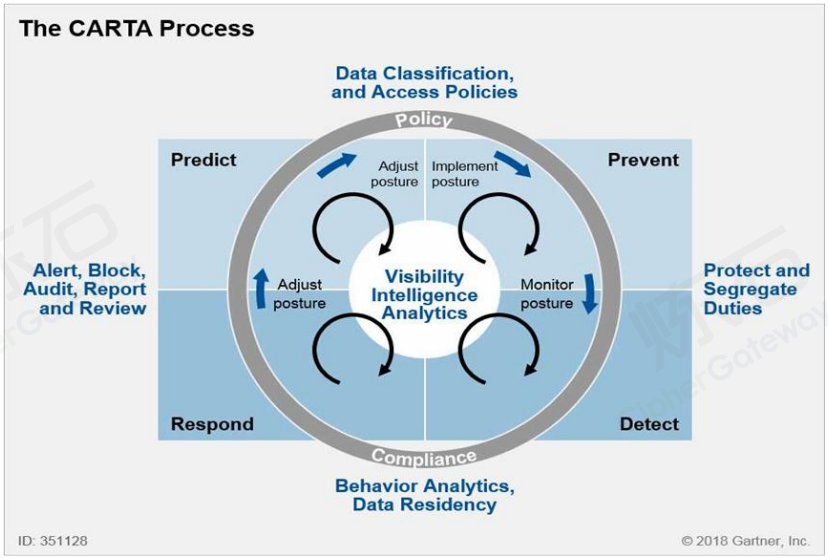

图 13 数字风险管理 CARTA 模型

预防阶段

1) 在所有存储位置发现数据至关重要。通过模式匹配和其他技术识别和分类数据的能力必须始终应用于结构化或非结构化格式的数据。单一产品很少能提供此功能，该产品还可以跨内部部署和跨公共云服务运行。并非所有数据都需要或应该存储；因此，积极计划将存储空间最小化。

2) 数据保护和匿名化选项包括加密，标记化，屏蔽或修订。但是，这些仅仅是访问控制，应用于强制执行职责分离（SOD）。它们可能具有多种功能来保护静止，使用中或运输中的数据，并可能有助于满足数据驻留和特定合规性要求。

检测阶段

1) 审查对关键数据集的访问权限，并为应用程序用户，开发人员，管理员和管理员的安全性实施 SOD。这需要仔细监视和限制特权，例如读取，

修改和删除。因此，仔细映射员工如何使用应用程序和分析产品来访问各种数据存储库。

2) 业务流程，身份和访问管理（IAM）和数据安全产品独立控制对数据的访问。因此，映射如何授予用户和管理员对数据集的访问权限，特权和权利。监视，识别和报告对访问，特权或权利的任何更改。

预测阶段

1) 为了完成该周期，必须针对安全映射练习所识别出的差距重新评估降低风险的选择。回顾行为分析输出可以帮助确定策略的粒度是否足够，例如，通过查看误报率以及检测恶意或不当行为的准确性来确定策略的粒度是否足够。

2) 审核日志是分析的重要来源，可用于识别策略规则漏洞和跨数据存储区的访问权限映射。合规性命令通常需要有关用户和管理员活动的审核报告。在安全事件或审核过程之后，将需要进行取证分析以检查日志。一些产品–例如安全信息和事件管理（SIEM）；安全运营，分析和报告（SOAR）；和安全运营中心（SOC）–可以提供日志的解释和创建；但是，他们缺乏数据活动的知识或洞察力。这需要以数据为中心的产品，例如数据丢失防护（DLP）和以数据为中心的审核和保护（DCAP）。

CARTA 模型四阶段——响应

1) 监视和分析用户行为的能力是了解和创建适当的安全响应的重要的第一步。使用异常或潜在恶意的数据监视和分析不断变化的特权和活动，并

警告管理员或数据所有者的相关安全性。或者，应用自动阻止响应以防止某些数据移动或活动，甚至是恶意软件的机器速度活动。

2) 了解数据如何跨地理管辖区流动对于了解需要更改策略规则或功能的数据驻留或合规性问题至关重要。

4.7.3.3 DGPC 框架

■ 基本概念

数据管治是对权限的规定和对数据资产管理的控制，即计划、监管和对数据管理的控制及使用。为保证隐私性、保密性和合规性所需的数据管治 Data Governance for Privacy, Confidentiality and Compliance（简称 DGPC）框架。旨在：

1) 保护组织数据，免受内部和外部威胁破坏隐私性和保密性

2) 确保组织遵从适用法、法规和标准

3) 确保在过程中生成合规性证据并存档。

DGPC 注重一系列技术和手动控制，以将安全性、隐私性和合规性风险维持在可接受的水平。这个方法涉及浏览考虑以下关键因素的风险管理流程：信息生命周期、组织的数据隐私和保密原则、内部策略以及四个特定的技术领域。

■ 主要实现

DGPC 框架围绕三个核心能力领域和三个标准

三个核心能力：人员、流程和技术

三个标准：IT 管理和控制框架（COBIT5.0 版本）、ISO/IEC27001/27002、支付卡行业数据安全标准（PCIDSS）

1) DGPC 在“人员”领域的控制要求

有效的数据安全治理要求建立适宜的组织架构和人员设置。DGPC 把数据安全相关的组织分为战略层、战术层和操作层三个层次，每一层次都要明确组织中的数据安全相关的角色职责、资源配置和操作指南。

图 14 DGPC 三层数据安全组织构架示意图

2) DGPC 在“流程”领域的控制要求

有了合适的组织和人员，组织就可以专注于定义所涉及的数据安全管理流程。首先检查数据安全相关的各种法规、标准、政策和程序，明确必须满足的要求，并使其制度化与流程化，以指导数据安全实践；组织应该在特定数据流的背景下，在制度和流程指导下，识别数据安全威胁、隐私风险和合规风险，并确定适当的控制目标和控制活动。

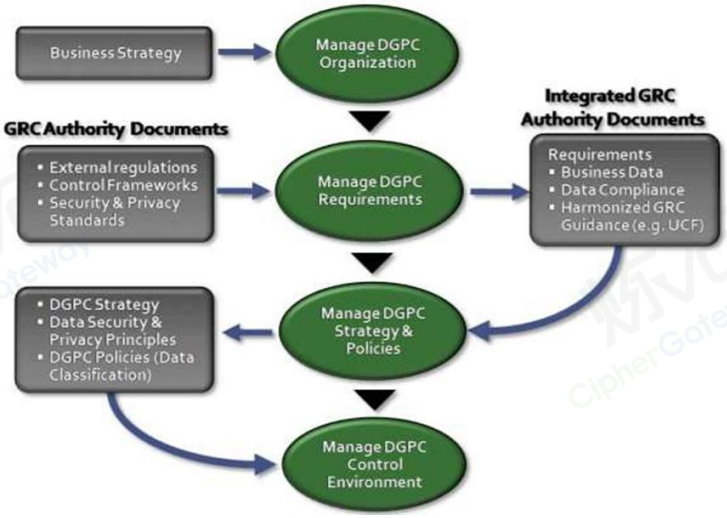

图 15 DGPC 数据安全管理流程图

3) DGPC 在“技术”领域的控制要求

Microsoft 开发了一种工具方法来分析与评估数据安全流程控制和技术控制存在的特定风险。这种方法需要填写一个称为安全差距分析表，该表围绕三个要素构建：信息生命周期，五种控制方法以及评估维度的数据隐私和保密原则。

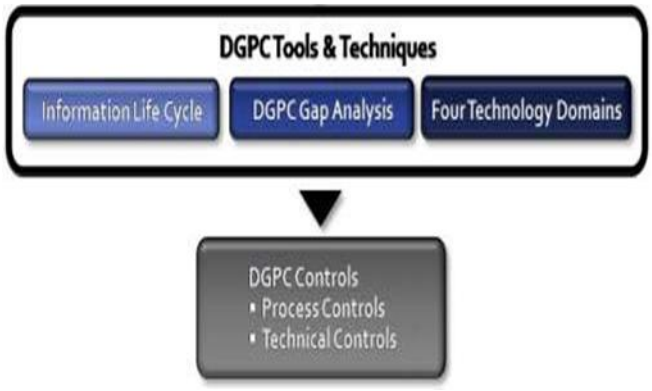

图 16 GPC 评估数据工具与技术示意图

4.7.3.4 FinDRA 模型

- 基本概念

数据使用带来的财务影响可以通过刚开发出来的 Gartner 新信息经济学模型来评估，即**财务数据风险评估（FinDRA）模型**。

■ 主要实现

财务数据风险评估（FinDRA）模型包括了五个处理步骤，如图所示：

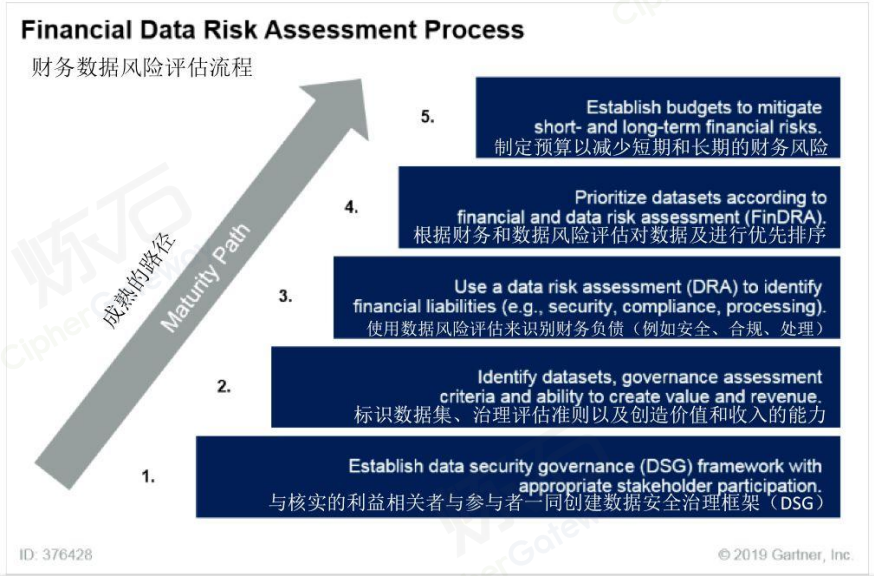

图 17 FinDRA 财务数据风险评估流程

4.7.4 数据安全管理

■ 基本概念

数据安全管理[103]是计划，制定，执行相关安全策略和规程，确保数据和信息资产在使用过程中有恰当的认证，授权等措施。

一般来讲，数据安全管理包含组织与人员、职责与分工、安全管理制度、安全技术手段等。本文由于篇幅问题，并考虑给读者提供直观的技术类治理手段，未包含组织、职责、管理制度等内容。

■ 主要实现

通常，针对数据安全管理工作，组织或企业需要考虑，实施“三评估、一平台，一评价”等重点工作，分别为：数据安全评估、隐私影响评估、个人信息安全影响评估、数据安全能力平台、数据安全能力评价等。

4.7.4.1 数据安全评估

结合定性分析和定量分析，分析和评估可能存在于产品、系统或工作中固有的或潜在的危险及其严重程度，并实施预防或防护策略，可以有效提升组织或企业安全性管理。

传统的，网络安全评估是网络安全风险管理中重要手段。数据安全评估由中国信息通信研究院发起进行系列电信网和互联网数据安全评估标准推动。

- 基本概念

数据安全评估[104]指结合企业组织机构、管理制度、技术能力等情况，运用科学的方法和手段，系统地对标我国数据安全相关政策法规和国家标准等要求，完整识别组织机构数据安全保护措施不到位情况，分析提出可能导致的数据安全风险，进而提出综合性和可操作性的防范对策、安全措施和改进建议。

- 主要实现

从通用性管理与全生命周期管理两方面出发，针对各个指标项，明确评估涉及的重要管理措施、重点技术措施及判断标准，明确被评估事项合规性保障基线，以提升企业数据安全管理及相关技术保障措施能力水平。

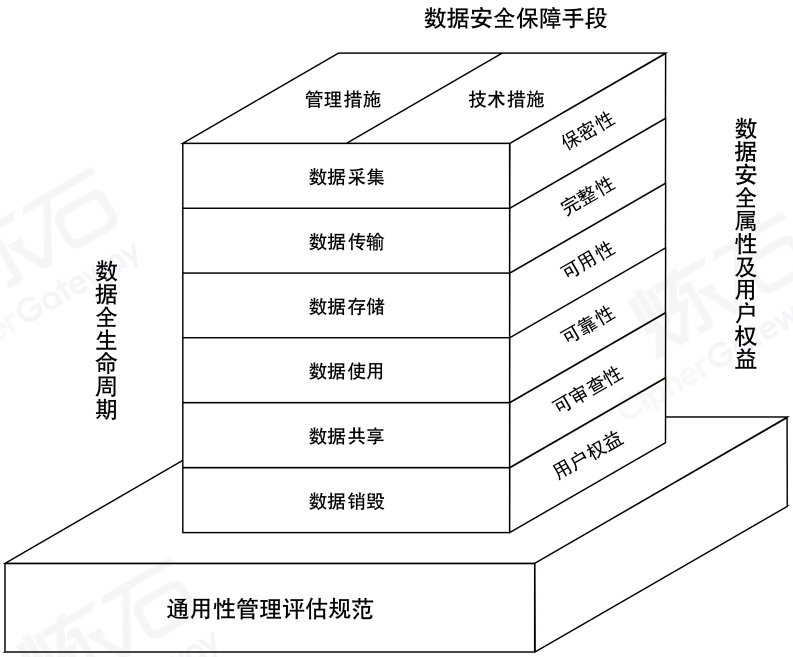

图 18 数据安全评估标准框架

评估基本流程包含评估准备阶段、评估实施阶段、评估总结阶段：

1）在评估准备阶段需要完成组建评估团队、确定评估范围、评估对象调研。

2）在评估实施阶段，对标数据安全基线要求，采用包括文档查验、人员访谈、系统演示、测评验证等方式对管理措施和技术措施进行评估，对不合规项逐项提出针对性整改建议。数据安全评估团队评估实践过程中，应当对评估佐证材料进行收集、整理，做好评估过程记录。评估实践过程通常可包括数据安全初评实践、数据安全复评实践。

3）在评估阶段，需要专家评审会，对评估实施过程及评估意见、评估整改落实情况进行核验，确认评估企业或评估对象是否已经配套数据安全管理措施和数据安全技术措施，满足数据安全基线要求，并撰写形成评估报告。

4.7.4.2 隐私影响评估

■ 基本概念

隐私影响评估指南（ISO/IEC 标准 29134）中，隐私影响评估（PIA）是一种评估流程，是评估信息系统，程序，软件模块，设备或其他处理个人身份信息(PII)的活动对隐私的潜在影响的工具，并与利益相关方协商，为治理隐私风险采取必要的行动。PIA 报告可能涵盖涉及风险治理措施的标准文件内容，包括因使用 ISO/IEC27001 标准中 ISMS（信息安全管理体系）而产生的措施。

■ 主要实现

隐私影响评估指南对 29134 实施进行指导，主要包含确定何时需要 PIA；编制 PIA 计划，如人员，资源、范围、利益相关方；识别信息流；识别、分析和评估隐私风险；实施风险处理计划和后续步骤；创建 PIA 报告。

4.7.4.3 个人信息安全影响评估

■ 基本概念

“个人信息安全影响评估”（personal information security impact assessment，简称“PISIA”），在《网络安全法》、《个人信息保护法（草案）》以及《数据安全法（草案）》中属于“风险评估”或者“安全评估”的范畴 1。根据《评估指南》[105]，“个人信息安全影响评估”是指针对个人信息处理活动，检验其合法合规程度，判断其对个人信息主体合法权益造成损害的各种风险，以及评估用于保护个人信息主体的各项措施有效性的过程。个人信息安全影响评估旨在发现、处置和持续监控个人信息处理过程中对个人信息主体合法权益造成不利影响的风险。

■ 主要实现

开展评估前，需要对评估的对象（可能为某项产品、某类业务、某项具体合作等）进行全面的调研，形成清晰的数据清单及数据映射图表（data flow charts），并梳理出待评估的具体的个人信息处理活动。

评估的规模往往取决于受到影响的个人信息主体范围、数量和受影响的程度。通常，企业在实施该类个人信息安全影响评估时，个人信息的类型、敏感程度、数量，涉及个人信息主体的范围和数量，以及能访问个人信息的人员范围等，都会成为影响评估规模的重要因素。

1) 评估必要性分析。包括合规差距评估、尽责性风险评估

2) 准备工作。包括组建评估团队、制定评估计划、确定评估对象和范围、咨询相关方，并制定评估计划。

3) 数据映射分析。在针对个人信息处理过程进行全面的调研后，形成清晰的数据清单及数据映射图表。需要结合个人信息处理的具体场景，开展方式可参考《评估指南》附录 C 中表 C.1《基于处理活动/场景/特性或组件的个人信息映射表》和 C.2《个人信息生命周期安全管理》

4) 风险源识别。对要素进行简化，归纳为网络环境和技术措施、个人信息处理流程、参与人员与第三方、业务特点和规模及安全趋势。

5) 个人权益影响分析。分析特定的个人信息处理活动是否会对个人信息主体合法权益产生影响，以及可能产生何种影响，主要包括四个维度：限制个人自主决定权、引发差别性待遇、个人名誉受损或遭受精神压力、

人身财产受损。可参考《评估指南》附录D.2《评估个人信息主体权益影响程度》。

6) 安全风险综合分析。评价安全事件发生的可能性等级，评价对个人权益影响的程度等级，综合考虑安全事件可能性和个人权益影响程度两个要素，综合分析得出个人信息处理活动的安全风险等级。

7) 评估报告。编制评估报告。个人信息安全影响评估报告的内容主要包括：评估所覆盖的业务场景、业务场景所涉及的具体的个人信息处理活动、负责及参与的部门和人员、已识别的风险、已采用及拟采用的安全控制措施清单、剩余风险等。

8) 风险处置和持续改进。通常情况下可根据风险的等级，采取立即处置、限期处置、权衡影响和成本后处置、接受风险等处置方式。

9) 制定报告发布策略。包括选取并实施安全控制措施，持续跟踪风险处置落实情况，评估剩余风险等。

4.7.4.4 数据安全能力平台

■ 基本概念

数据安全治理工作是战略性投入，成效需要长期跟踪为有明显效果。数据安全能力平台指协助数据安全从业者或监管者开展数据安全相关工作，实现平台、工具、流程、机制有效结合，提升工作效率。

■ 主要实现

常见的数据安全能力平台包含但不限于数据安全管控平台、数据安全治理系统、SaaS 平台安全管理、工业安全智能监管平台、容器安全管理系统、云安全资源池等。

 # 数据安全管控平台

数据安全管控平台整合数据资源安全运营、数据安全策略运营、数据安全事件运营、数据安全风险运营，通过数据发现、策略管控、事件监测、风险分析等能力管控等，实现对组织的数据安全管控工作的信息化支撑。

 # 数据安全治理系统

数据安全合规矩阵由控制矩阵、检查矩阵、责任矩阵组成，在充分采纳和吸收 G.R.C 管理基础上，解析组织面临数据安全制度与规范，同时借鉴国内、国际成熟最佳实践，实现数据安全合规治理体系化，并将数据安全要求落实到岗到人（职责落地）。

 # SaaS 安全管理平台

Gartner 将 SaaS 安全态势管理（SSPM）定义为持续评估安全风险和管理 SaaS 应用程序安全态势的工具。核心功能包括报告本地 SaaS 安全设置的配置，并提供改进配置以降低风险的建议。

另外一个较为精准定义：一组自动化的安全工具和自动化工具，使组织的安全和 IT 团队能够了解并管理其 SaaS 环境的安全态势。

 # 容器安全管理系统

通过容器资产发现、安全可视化、嵌入 DevOps 等方式，为用户提供资产管理、镜像安全、集群合规、运行安全、容器微隔离等功能，实现对容器全生命周期的自动化安全管理。

4.7.4.5 数据安全能力评价

数据安全概念在多元素作用下，不断昨到监管、需求、供给各方认可。对于具体一个企业或者组织,数据安全工作可能是由网络安全层面不断进行数据安全增强，或者主抓重点或者从数据源发现开展，都需要持续性关注并不断验证。数据安全评价是数据安全管理重点工作之一，是形成整个闭环管理的关键环节。

- 基本概念

根据《信息安全技术数据安全能力成熟度模型》，通过在组织机构业务场景中的数据生命周期，从组织建设、制度流程、技术工具以及人员能力四个方面构建了数据安全过程的规范性数据安全能力成熟度分级模型及其评估方法。

《信息安全技术数据安全能力成熟度模型》[106]参考能力成熟度模型（CMM）的思想，以 CMM 的通用实践来衡量能力成熟度等级，以《信息安全技术大数据服务安全能力要求》中的安全要求为基础，指导组织机构如何持续达到所对应的安全要求。数据安全能力成熟度模型的模型架构由以下三方面构成：

——数据生命周期安全：围绕数据生命周期，提炼出大数据环境下，以数据为中心，针对数据生命周期各阶段建立的相关数据安全过程域体系。

——安全能力维度：明确组织机构在各数据安全领域所需要具备的能力维度，明确为制度流程、人员能力、组织建设和技术工具四个关键能力的维度。

——能力成熟度等级：基于统一的分级标准，细化组织机构在各数据安全过程域的5个级别的能力成熟度分级要求。

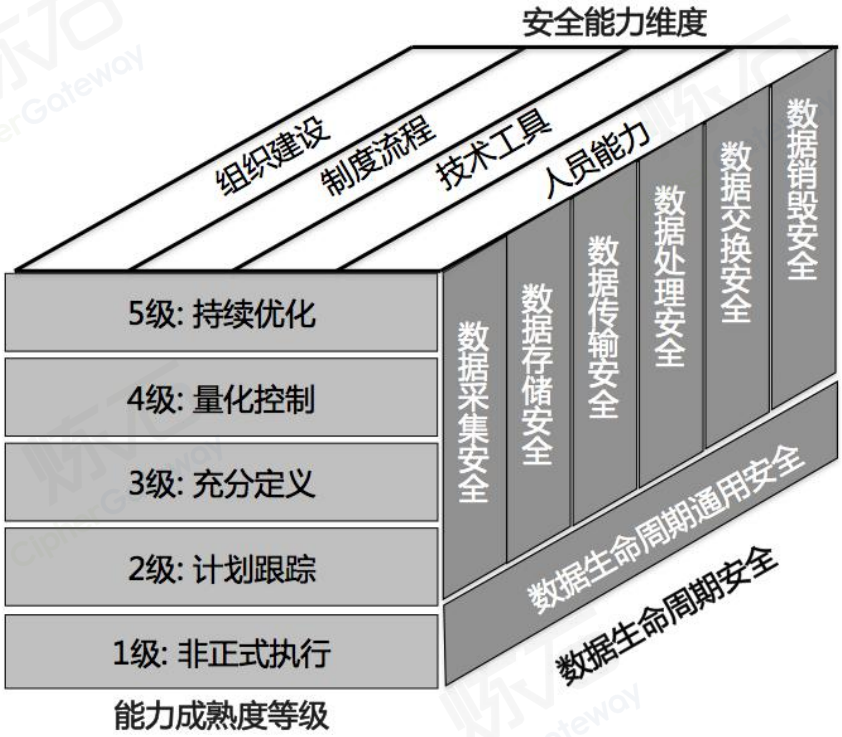

图 19 成熟度模型

■ 主要实现

数据安全能力成熟度模型能力维度包含组织建设、制度流程、技术工具及人员能力四个维度。

1) 组织建设

从承担数据安全工作的组织机构建设应具备的能力出发，从以下方面进行能力的级别区分：

——数据安全组织架构对组织业务的适用性；

——数据安全组织机构承担的工作职责的明确性；

——数据安全组织机构运作、沟通协调的有效性。

2) 制度流程

从组织机构在数据安全层面的制度流程建设，以及制度流程的执行情况出发，从以下维度进行能力的级别区分：

——数据生命周期关键控制节点授权审批流程的明确性；

——相关流程制度的制定、发布、修订的规范性；

——安全要求及流程落地执行的一致性和有效性。

3) 技术工具

从组织机构用于开展数据安全工作的安全技术、应用系统和自动化工具出发，从以下维度进行能力的级别区分：

——数据安全技术在数据全生命周期过程中的利用情况，针对数据全生命周期安全风险的检测及响应能力；

——利用技术工具对数据安全工作的自动化支持能力，对数据安全制度流程的固化执行能力。

4) 人员能力

从组织机构内部承担数据安全工作的人员应具备的能力出发，从以下维度进行能力的级别区分：

——数据安全人员所具备的数据安全能力是否能够满足复合型能力要求(对数据相关业务的理解力以及专业安全能力);

——数据安全人员的数据安全意识以及关键数据安全岗位员工的数据安全能力的培养。

4.7.5 数据安全运营

4.7.5.1DataOps

■ 基本概念

根据维基百科，DataOps（数据运维）指一种面向流程的自动化方法，由分析和数据团队使用，旨在提高数据分析的质量并缩短数据分析的周期。

根据 MicheleGoetz[24]，DataOps（数据运维）指基础设施到体验的所有技术层，实现解决方案，开发数据产品以及激活数据以实现商业价值的能力。

■ 主要实现

从搭建基础架构到使用数据应用的结果，通常需要实现以下功能。

1) 部署：包括基础架构和应用程序。无论底层硬件基础设施如何，配置新系统环境都应该快速而简单。部署新应用程序应该花费几秒而不是几小时或几天时间。

2) 运维：系统和应用程序的可扩展性、可用性、监控、恢复和可靠性。数据应用开发人员不必担心运维，可以专注于业务逻辑。

3) 治理：数据的安全性、质量和完整性，包括审计和访问控制。所有数据都在一个支持多租户的安全环境中以连贯和受控的方式进行管理。

4) 可用：用户应该能够选择他们想要用于数据开发和分析的工具，随时拿到他们可用的数据，并根据需要轻松开发和运行数据分析应用。应将对不同分析、ML、AI 框架的支持整合到系统中。

5) 生产：通过调度和数据监控，可以轻松地将分析程序转换为生产应用，构建从数据抽取到数据分析的生产级数据流水线，并且数据应该易于使用并由系统管理。

要构建 DataOps 所需的通用平台，一般需要以下技术。

 # 云架构

必须使用基于云的基础架构来支持资源管理、可扩展性和运营效率。

 # 容器

容器在 DevOps 的实现中至关重要，在资源隔离和提供一致开发、测试、运维环境中的作用也至关重要。

 # 时和流处理

目前来看，实时和流处理在数据驱动平台中变得越来越重要，它们应该是现代数据平台中的“一等公民”。

 # 多分析引擎

MapReduce 是传统的分布式处理框架，但 Spark 和 TensorFlow 等框架日常使用越来越广泛，应该进行集成。

 # 集成的应用程序和数据管理

应用程序和数据管理（包括生命周期管理、调度、监控、日志记录支持）对于生产数据平台至关重要。DevOps 的常规实践可应用于应用程序管理，但是数据管理及应用程序与数据之间的交互需要很多额外的工作。

 # 多租户和安全性

数据安全性可以说是数据项目中最重要的问题，如果数据无法得到保护，数据使用也就无从谈起。该平台应为每个人提供一个安全的环境，使每个人都可以使用这些数据并对每个操作进行授权、验证和审核。

 # DevOps 工具

数据科学家提供有效的工具，以分析数据并生成分析程序，为数据工程师提供大数据流水线的工具，并为其他人提供消费数据和结果的方法。

4.7.5.2DevOps

- 基本概念

根据维基百科定义，DevOps（开发安，Development 和 Operations 的组合词）是指一种重视“软件开发人员（Dev）”和“IT 运维技术人员（Ops）”之间沟通合作的文化、运动或惯例。透过自动化“软件交付”和“架构变更”的流程，来使得构建、测试、发布软件能够更加地快捷、频繁和可靠。

- 主要实现

DevOps 的引入能对产品交付、测试、功能开发和维护（包括——曾经罕见但如今已屡见不鲜的——“热补丁”）起到意义深远的影响[34]。通常，实施 DevOps 主要包含如下几下过程：

1.确定业务理由。

2.为所在企业定义 DevOps

3.选择“先行者”应用软件

4.确定初始团队

5.确立目标和度量指标

6.专注于限制因素

7.开发工具链

8.准备好后扩展

4.7.5.3 供应链安全[101]

供应链系统，在当今环境复杂、需求多样、竞争激烈的市场经济背景下，其供应链的多头主体的参与、跨地域、多环节的特征，使供应链系统容易受到来自外部和链条上各自实体内部不利因素的影响，就会客观地形成供应链风险。

据魏昊总结：供应链安全存在以下四个方面的主要风险：

1) 网络产品和服务自身安全风险，以及被非法控制、干扰和中断运行的风险；

[34]DevOps 可以优化组织中开发、运营、业务、用户之间信息鸿沟。

2) 网络产品及关键部件生产、测试、交付、技术支持过程中的供应链安全风险；

3) 网络产品和服务提供者利用提供产品和服务的便利条件非法收集、存储、处理、使用用户相关信息的风险；

4) 网络产品和服务提供者利用用户对产品和服务的依赖，损害网络安全和用户利益的风险。

■ 基本概念

供应链安全是保护供应链免受各种威胁的损害，以确保业务连续性，业务风险最小化，投资回报和商业机遇最大化。

■ 主要实现

根据《供应链安全分析》[100]，企业可考虑从如下层面，做好供应链安全。

1) 在供应链构建初期，充分考虑到风险问题，提高整体安全防范意识；

2) 加大供应链信息共享，有效促进各主体间的安全防范工作开展；

3) 加强客户与供应商的关系管理，选择可靠的供应商，构建诚信合作体系；

4) 逐步推行产品及服务的国产化，尽量避免国际形势带来的安全风险；

5) 制定突发事件的应急措施，加强企业应急响应能力；

6) 充分利用高新技术，提高企业安全防御能力。

根据《数据安全下的供应链管理建设》[102]，考虑 DSMM 框架构建供应链安全体系，如下：

图 20 DSMM 框架构建供应链安全体系

4.7.6 意识与教育

理想情况下，充分的安全保护技术和完善安全管理制度可以解决我们面临的数据安全问题，但是业务和数据本身服务于人，安全措施也需要人来驱动。人是“数据”的周边环境中最大的可变因素。加强人的安全意识与技术，可能极大减少安全事件发生。

■ 基本概念

数据安全意识与信息安全意识类似，指人们头脑中建立起来的信息化和数字化工作必须安全的观念，也就是人们在信息化和数字化工作中对各种各样有可能对信息和数据本身或信息数据所处的介质造成损害的外在条件的一种戒备和警觉的心理状态。

数据安全教育，指帮助安全人员、业务人员学习数据安全知识，提高安全意识和安全防护能力，满足组织或企业数据安全的要求，适应数据安全和个人信息保护不断发展的需求。

■ 主要实现

通过安全意识动画、安全意识画册、安全意识海报、安全意识屏保、安全意识电子期刊等提升数据安全意识；通过理论知识和管理方法论学习，夯实数据安全理论知识；通过案例讲演、攻防实操，提升员工数据安全操作能力。

4.7.7 数字道德

各种数据安全事件，让所有人明白一个道理：人类文明仍然在道德范畴内活动。本文把数字道德放置于整个 DTTACK 框架最后一部分，旨在强调用道德约束来总结整个框架。

- 基本概念

数字道德（又称数字化道德，数字伦理）强调利用责任感的承诺，约束数据化技术不损害国家安全、社会稳定和个人权益，进而保障客户、员工和投资者利益。

数字伦理维基百科定义为伦理的一个分支，关注信息的创造、组织、传播和使用与管理信息的伦理标准和道德规范之间的关系。

数字道德常见内容涉及知识产权、隐私、安全、信息过载、数字鸿沟、性别歧视和审查等。

- 主要实现

通常，考虑将数字道德融入到企业的组织结构和业务流程中，将数字道德重点因素与管理架构、绩效指标和安全审查相结合，并优化业务流程，让数字道德在人员、技术、操作多方面发挥作用。

AvanadeTrendlines：数字道德

实施数字伦理是一个变革管理进程；像一个人一样对待，具有多种形式的培训，激励和加强行为变革。重点包含公平和包容性（需要识别和曝光等数字系统中的偏见）；人的责任（建立信任，最大限度地减少伤害，并确保在创新过程中的每个重要里程碑处进行人工干预和检查）；适用性（必须设计和测试数字系统，以确保应急响应）；安全地响应意外的情况，并不会以与原始期望不一致的方式发展。值得信赖性（明示告知，明示同意）。

图 21 AvanadeTrendlines 数字道德的四个要点

Gartner：数字道德与隐私

Gartner 数字道德[98][99]定义范围较广，包含安全、网络犯罪、隐私、社会互动、治理和自由意志以及社会和整个经济。数字道德与隐私强调，合规性最基本满足项；风险控制在组织可承受级别；利用数字道德的价值主张来实现差异化竞争；组织层的道德驱动，整体框架[15-16]如下图所示：

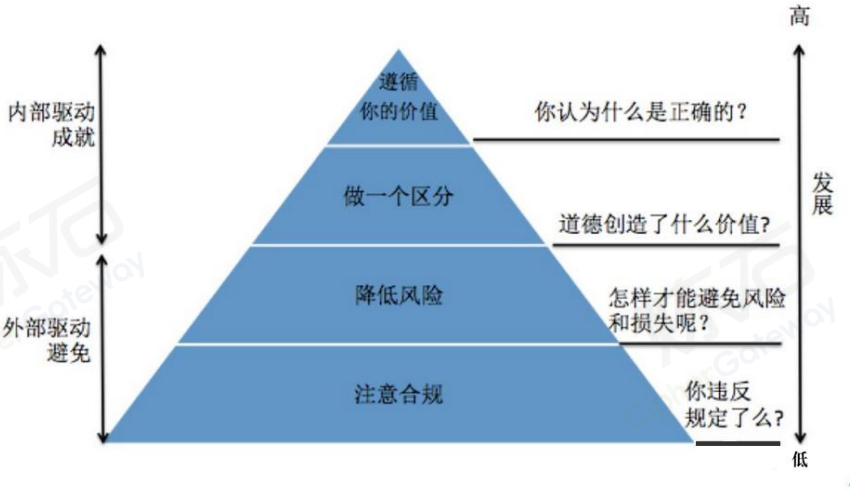

图 22 Gartner 数字道德与隐私

五、数据安全应用示例方案参考

5.1 云平台数据安全存储场景

参考适用场景：云平台中数据存储场景

表 1 云平台数据安全存储场景典型威胁情境

主体	路径与客体	意图与结果
黑客或应用程序、数据库、主机、存储运营人员	运维应用或设备，非授权访问敏感数据	① 恶意窃取数据
第三方，如黑客、网络爬虫、互联网探测平台等	访问控制失效敏感数据被暴露	恶意或非恶意访问并泄露或公开敏感数据

5.1.1 概要

把企业业务和数据托管于云服务，即可以降低硬件采购成本，又可以减少运维成本。同时，云端资源可实现高弹性和个性化订制服务。但是对于企业用户来说，由于网络、业务、数据由第三方来负责维护，那么数据是否可能被未知的超级用户访问，是否可能被异常丢失、数据泄露[35]，一直困扰着已上云或计划上去企业用户。

同时，根据《中华人民共和国网络安全法》第二十一条要求：网络运营者应当按照网络安全等级保护制度的要求进行网络安全保护，网络运营者不履行等保义务的，将被给予警告并处以罚款，构成犯罪的，依法追究刑事责任。结合等级保护 2.0 云计算扩展要求，企业不管是整体或部分业务迁移到云端都要保证安全

[35] 据 RedLock 公司调研报告中 AWS S3 的企业用户，如道琼斯、威瑞森、联邦快递和特斯拉等公司都遭遇了云端数据泄露事件。2019 年 11 月，浙江省通信管理局责令阿里云整改关于未经用户同意擅自将用户留存的注册信息泄露给第三方合作公司的事件。

合规。

5.1.2 安全现状

5.1.2.1 已完成安全建设

目前，国内主流的云服务商都通过三级及以上等保测评，满足A类机房要求，具备27001等国内国际安全认证。同时，大多数云服务商都具备安全能力云服务，如DDoS流量清洗、漏洞扫描、Web应用防火墙、云证书管理、SSL证书管理、云堡垒机等，等级保护建设涉及软硬件安全设备。同时，在预算可控条件下，云租户会采购配套的等级保护咨询和测评服务。

5.1.2.2 缺失安全手段

业务上云后，企业面临最突出安全问题是安全边界被打破。大量的数据异地存储和使用，现有的多数安全手段更加注重于网络边界防护和访问控制。但云上存储的数据可能存在明文数据泄露的风险。企业应该考虑利用加密、去标识化技术为云上高速流转的数据重构防护边界。

需要解决如下数据安全风险：

1. 数据存储安全风险：存储在云端的数据可能被黑客攻击应用引发数据泄露，可能被数据库运维人员攻击数据库引发数据泄露，可能被虚拟机运维人员攻击引发数据泄露，可能被存储管理人员攻击引发数据泄露。

2. 访问控制失造成数据泄露风险：云服务中安全配合至关重要，默认口令/弱口令、应用配置文件非授权访问等都有可能被第三方或黑客网络爬虫、互联网探测平台等，恶意或非恶意访问并泄露或公开。

3. 法律合规遵循不足风险：较多企业在系统或业务定级备案时，未充分关注云上业务或数据满足等保合规及信息系统密码应用基本要求的管理规定。

5.1.3 解决方案

建议平台管理者单位结合 DTTACK 模型，进行如下方案分析与设计：

需求一实现：选择 4.2 P:防护^4.2.1 技术：数据加密技术^4.2.1.1 扩展技术：存储加密^# 应用内加密（AOE 面向切面加密）方法；选择 4.2 P:防护^4.2.9 技术：云数据保护技术^4.2.9.1 扩展技术：云密码服务^# 密钥管理；选择 4.2 P:防护^4.2.1 技术：数据加密技术^4.2.1.1 扩展技术：存储加密^# TFE 透明文件加密；选择# FDE 全磁盘加密。

需求二实现：选择 4.2 P:防护^4.2.5 技术：访问控制^4.2.5.2 扩展技术：权限管理控制^# RBAC 技术；选择# ABAC 技术，选择# ABAC 技术；选择 4.2 P:防护^4.2.4 技术：身份认证技术^4.2.4.3 扩展技术：生物特征认证技术；选择 4.2 P:防护^4.2.6 技术：数字签名^4.2.6.2 扩展技术：签名验签技术；选择 4.7 G:治理^4.7.7 数字道德^# AvanadeTrendlines：数字道德技术。

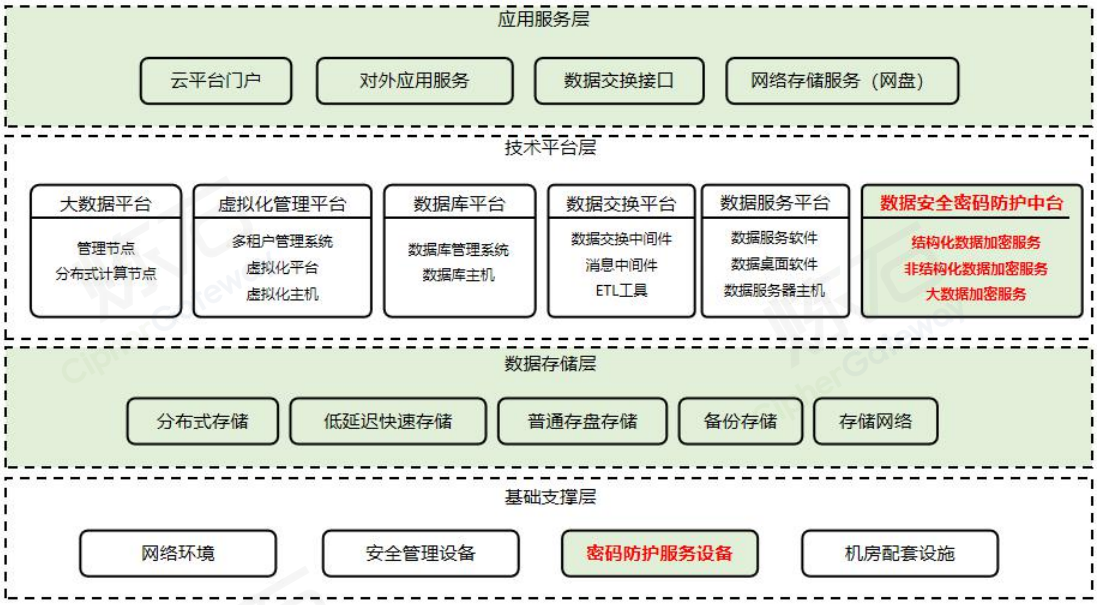

图 23 加入密码能力支撑的云平台整体规划

建设以密码技术为核心的数据安全密码防护中台，以应用层为抓手，可实现：

1.云平台上的数据加密存储，防范数据泄露风险；

2.云平台上的应用系统可免开发改造，敏捷实施，成本低；

3.提供云服务形态，对存量和新增应用增强密码防护能力；

4.满足等保合规及信息系统密码应用基本要求的管理规定。

5.1.4 总结

企业将系统或数据迁移到云平台可能存在数据被泄露、被滥用等安全风险，通过构建密码基础设施和密码服务平台，强化生物识别或证书登录，使用密码技术实现用户身份鉴别、应用程序访问控制、数据存储过机密性和完整性保护，进一步满足等保 2.0 以及密码应用安全性评估等合规要求。

5.2 工业互联网数据多方安全共享

参考适用场景：工业数据、制造业数据在多个参与方进行数据共享时数据安全实现。

表 2 工业互联网数据多方安全共享场景典型威胁情境

主体	路径与客体	意图与结果
数据共享参与方	在数据共享方案中，泄露参与方身份信息	非恶意获得权限以外的原始敏感数据
数据共享参与方	在数据共享方案中，泄露参与方敏感数据	非恶意获得权限以外的原始敏感数据

5.2.1 概要

利用工业互联网新技术、新应用，对传统产业进行全方位、全角度、全链条的改造，提高全要素生产率，释放数字对经济发展的放大、叠加、倍增效应。数据是工业互联网的核心，在工业互联网中，汇聚着海量来自不同工业运营商数据尽管如此，随着工业数据由少量、单一、单向正在向大量、多维、双向转变，具体表现为工业互联网数据体量大、种类多、结构复杂。工业领域业务应用复杂，数据种类和保护需求多样，数据流动方向和路径复杂，重要工业数据以及用户数据保护的难度陡然增大。

5.2.2 安全现状

5.2.2.1 已完成安全建设

工业互联网相关企业在信息化规划及建设规划过程中都已或多或少考虑了信息安全，并已经建立了一些信息安全系统，企业信息安全系统主要由防火墙、VPN、IPS、IDS、防病毒、存储备份、容灾和安全管理制度等组成。

在工业互联网数据共享交换场景下,由国家监管部门大力支持下已经在预研了通用计算服务平台，平台设计具有去中心化、数据保护、联合计算等功能。

5.2.2.2 缺失安全手段

在进行企业内部和外部进行数据共享交换时，没有充分的数据安全措施，面临着更多的数据交换方式和业务应用方式的结合问题。同时，工业网络接入互联网已势在必行，在完善的计算服务平台未推广或形成快捷解决方案时，需要进行紧急数据安全手段补充，其中建设重点和难点在于：

1. 通过算法自动化智能化的发现数据平台中存在的敏感数据；

2. 敏感数据动态脱敏，在客户端和服务器之间按照策略进行SQL操作的改写，来实现对数据脱敏的效果；

3. 加密特定的文件类型(例如电子表格、数据库、文件或临时文件夹)；

4.在传统的访问控制基础上，实现主体到人，客体到字段的动态、精细化的访问控制；

5.对敏感数据，如调度数据、交付日期、机器的状态数据和运维状态、产品的供应状态、源代码、图纸等，实现多方安全计算，以防止数据安全和其他安全风险失控。

5.2.3 解决方案

建议企业管理者单位结合 DTTACK 模型，进行如下方案分析与设计：

需求一实现：选择 4.3 D:检测^44.3.5 技术：共享监控^4.3.5.3 扩展技术：接口访问预警^# 文字识别技术；选择# 图片识别技术。

需求二实现：选择 4.2 P:防护^4.2.1 技术：数据加密技术^4.2.1.1 扩展技术：存储加密^# 应用内加密（AOE 面向切面加密）方法；针对工业互产网数据类型，筛选并建立行业敏感字段（主要参考《工业数据分类分级指南（试行）》、《工业数据质量—通用技术规范》（GB/T 39400-2020）、《T/31SCTA 003-2017 工业大数据平台技术规范 数据处理》等）、数据库字段等特征库；利用脱敏模块实现敏感字段的字段级加密。

需求三实现：选择 4.2 P:防护^4.2.1 技术：数据加密技术^4.2.1.1 扩展技术：存储加密^# 应用内加密（AOE 面向切面加密）方法。

需求四实现：选择 4.2 P:防护^4.2.5 技术：访问控制^4.2.5.2 扩展技术：权限管理控制^# ABAC 技术。

需求五实现：选择 4.2 P:防护^4.2.1 技术：数据加密技术^4.2.1.3 扩展技术：使用加密^# MPC 多方安全计算技术。

具体地：

1. 采用 TFE 透明文件加密

对指定类型的文件进行实时、强制、透明的加解密，在正常使用时，计算机内存中的文件是以受保护的明文形式存放，但硬盘上保存的数据却处于加密状态，如果没有合法的使用身份、访问权限和正确的安全通道，所有加密文件都将以密文状态保存。

2. 采用应用级存储加密技术

通过 AOE 面向切面加密技术对应用程序产生的敏感数据进行加密。

1）将 AOE 模块部署在客户应用服务器上，数据经应用采集，插入到数据库时，模块会根据设置的加密策略将数据加密，以密文形式存储在应用所连接的数据库上。

2）当数据从应用端被访问时被解密，并根据所设置的脱敏策略在应用端展示脱敏后的数据或明文数据。

3. ABAC（基于属性的访问控制）功能

实现主体到人，客体到字段的动态态、精细化的访问控制。通过管理平台对企业员工进行权限管理。其中，访问主体的用户信息可以与企业的统一用户身份管理进行集成，也可以与应用的用户管理进行同步。在密文数据被访问时，则根据用户身份，向授权的用户展示明文数据或部分遮掩数据，而向未授权用户展示密文或脱敏数据。实现结合用户身份的动态脱敏，保证对于敏感数据的严格管控，并支持可追溯、防篡改的第三方数据操作审计，每条日志支持主体追溯到人，保证可事后追责。

5.2.4 总结

分析工业互联网企业数据防泄密路径和数据共享交换业务特性，利用加密技术、去标识化技术、多方安全计算技术保护企业的信息资产和核心机密数据为企业提供有效的数据安全保障。

5.3 重要商业设计图纸安全共享场景

参考适用场景：商业秘密在组织内部人员间合法加工、使用场景

表 3 重要商业设计图纸安全共享场景典型威胁情境

主体	路径与客体	意图与结果
内部工作人员	日常办公使用商业秘密数据	② 非故意终端遗失，造成数据被公开或买卖 ③ 线下使用秘密数据，恶意或非恶意造成影印文件丢失
第三方人员或内部技术人员或黑客	维护文件服务；非法访问文件服务器	滥用权限或恶意攻击，获取原始敏感数据

5.3.1 概要

有色矿山经营活动中涉及的采矿方法、采掘工程设计、竖井设计等商业秘密，是整个企业智力独创性成果。在设计过程中，投入多、独创性强，价值亦很高。同时,在设计过程中必然会产生大量的信息和数据,并最终形成重要的设计成果。一旦设计成果被非法泄露，将会对有色矿山单位产生重大的影响。

5.3.2 安全现状

5.3.2.1 已完成安全建设

有色矿山中重要商业设计图纸本身为受限传播。日常工作中，通过安全意识提升和管理手段来加强数据保护。在重要图纸对外传播中，设计有严格的管理流程，实现层层审批。

5.3.2.2 缺失安全手段

近年，从勒索病毒到心血漏洞，无不表明安全攻击无处不在，从谷歌程序员泄露数据到设计公司员工离职窃取公司设计图纸,无不表明内外安全防护同等重要。重要商业设计图纸是企业运营数据，是有色矿山核心资产，必须做到万无一失。

有色矿山中重要商业设计图纸数据需要紧急解决如下数据安全风险：

1. 实现员工固定办公终端和移动办公终端数据保护，解决一线员工、管理层使用图纸便利性和数据安全性问题，特别解决办公终端失窃带来安全隐患；

2. 重要商业设计图纸在管理层传递时，敏感信息外传风险，实现针对重要图纸对外非授权展示或传播管控；

3. 在存储服务器内，实现重要图纸加密存储和访问控制减少内部技术人员和黑客获取原始文件风险；

4. 在重要商业设计图纸组织内部线下传递时，实现流转控制，防止影印文件流失。

5.3.3 解决方案

建议企业管理者单位结合 DTTACK 模型，进行如下方案分析与设计：

需求一实现：选择 4.2 P:防护^4.2.1 技术：数据加密技术^4.2.1.1 扩展技术：存储加密^# FDE 全磁盘加密方法；选择 4.2 P:防护^4.2.9 技术：云数据保护技术

^4.2.9.1 扩展技术：云密码服务^# 密钥管理；选择 4.2 P:防护^4.2.5 技术：访问控制^4.2.5.4 扩展技术：数据访问控制^# 存储介质访问控制技术；

需求二实现：选择 4.6 C:反制^4.6.1 技术：水印技术^4.6.1.4 扩展技术：屏幕水印技术；选择 4.2 P:防护^4.2.5 技术：访问控制^4.2.5.4 扩展技术：数据访问控制^# 存储介质访问控制技术；

需求三实现：选择 4.2 P:防护^4.2.1 技术：数据加密技术^4.2.1.1 扩展技术：存储加密^# TFE 透明文件加密方法；

需求四实现：选择 4.6 C:反制^4.6.1 技术：水印技术^4.6.1.2 扩展技术：多媒体水印技术；选择 4.7 G:治理^4.7.7 数字道德^# AvanadeTrendlines：数字道德技术。

整体安全增强设计如下图所示：

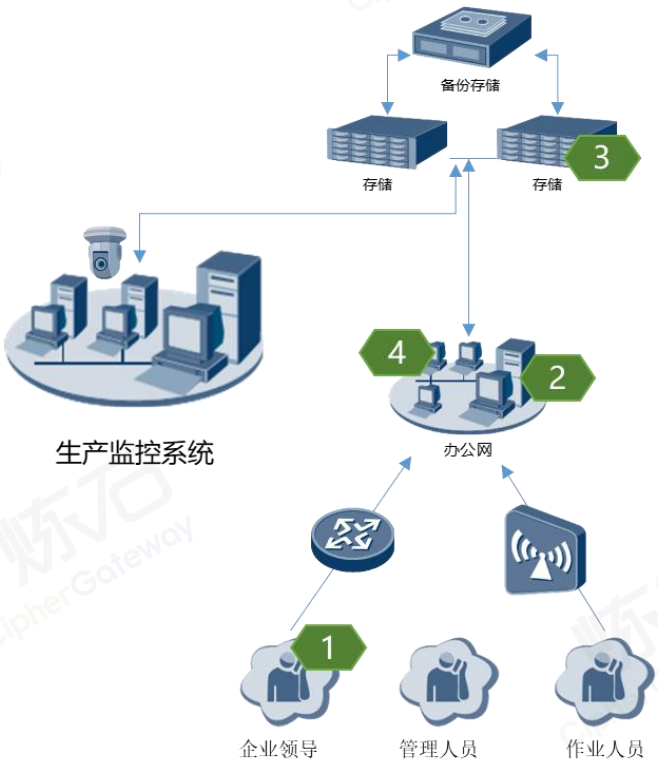

图 24 重要商业设计图纸安全共享使用解决方案

在增强点 1，在企业领导侧安装 FDE 以及终端控制或终端准入（身份认证）软件；在办公网部署密钥管理系统（硬件）。

在增强点 2，在业务分析系统或生产管控系统增加屏幕水印功能，实现使用者身份特征嵌入，威慑内部人员泄露敏感数据情形。

在增强点 3，在存储服务器以及备份存储服务器上部署 TFE 加密模块，实现敏感图纸文件存储层加密保护。

在增强点 4，在打印机添加或开启打印机水印功能（配合接入设备管理），并通过日常管理工作增加安全意识宣贯。

5.3.4 总结

传统地，重要商业设计图纸传递和使用受限于信息化有段，面临的数据安全风险较小。随着，智能化矿山建设，大量的办公设备接入矿山信息化系统，特别地，移动办公终端的使用导致信息可以被非法传播，被滥用，被窃取等。根据当前管理层以及一线员工层对数据管控难点和痛点，利用 DTTACK 模型，选择适宜的技术方案，实现安全风险缓解基础上，保证业务可用和易用。

5.4 电子档案数据的安全存储和使用场景

参考适用场景：电子档案数据安全存储和使用安全场景

表 4 电子档案数据的安全存储和使用场景典型威胁情境

主体	路径与客体	意图与结果

第三方人员或内部技术人员或黑客	维护文件服务;非法访问文件服务器	滥用权限或恶意攻击,获取原始敏感数据

5.4.1 概要

根据《中华人民共和国档案法》第三十七条要求，电子档案应当来源可靠、程序规范、要素合规。电子档案成为各级政府以及档案馆的重要工作之一。同时，2018 年国家档案局发布了《电子档案管理系统基本功能规定》，进一步规范了电子档案管理系统建设要求，电子档案的移交接收、长期保存、共享利用和安全可靠等是基本的业务需求。

电子档案的数量呈现指数级增加，从而关于电子档案安全问题，特别是数据安全问题成为关注热点。电子档案载体的完整性和可用性，以及存储安全性和传输安全性成为重点解决难题。

5.4.2 安全现状

5.4.2.1 已完成安全建设

遵循国家档案局办公室关于《档案信息系统安全等级保护定级工作指南》，档案信息管理系统、档案信息服务系统、档案办公系统已经实现了充分的网络安全保护，如：（1）身份认证和用户权限管理；（2）部署了防火墙和入侵检测系统。（3）实现了数据与系统备份。

5.4.2.2 缺失安全手段

档案数字化的快速推进，智慧电子档案系统存在的主要安全风险表现在：档案失密泄密风险，包括计算机、服务器等在内的档案系统的载体是确保数字化档

案安全的基础。现有的档案以明文进行存储、系统面临着黑客攻击、破解等导致的受损或丢失风险。

组织的档案管理中需要紧急解决如下数据安全风险：

1. 档案的明文存储造成数据泄露或非法访问；

2. 档案数据操作安全审计不足，如用户登录及访问信息、档案操作情况（如检索、调阅、增删、查改），不能及时发现违规操作行为。

5.4.3 解决方案

建议企业管理者单位结合 DTTACK 模型，进行如下方案分析与设计：

需求一实现：选择 4.2 P:防护^4.2.1 技术：数据加密技术^4.2.1.1 扩展技术：存储加密^# TFE 全磁盘加密方法；选择 4.2 P:防护^4.2.9 技术：云数据保护技术^4.2.9.1 扩展技术：云密码服务^# 密钥管理；

需求二实现：选择 4.3 D:检测^4.3.4 技术：安全审计^4.3.4.4 扩展技术：业务安全审计方法。

具体地，采用 TFE 透明文件加密。

TFE 模块在操作系统层对非结构化数据（文档、图片、音频、视频等）进行加解密，与文件管理平台交互，根据获取的加解密策略，对文件进行加解密，并且可以“逐文件逐密钥”对数据进行更要求的安全防护。

文件在计算机内存中时是以受保护的明文形式存放，加密后以密文落盘存储。数据安全审计。通过数据安全管理平台对企业员工进行权限管理。其中，访问主体的用户信息可以与企业的统一用户身份管理进行集成，也可以与应用的用

户管理进行同步。把访问日志保存下来，支持可追溯、防篡改的第三方数据操作审计，每条日志支持主体追溯到人，保证可事后追责。

5.4.4 总结

传统的档案管理系统大多因信息安全防护能力不足而普遍存在权限滥用、信息泄露等安全风险。通过数据加密技术和数据安全审计技术等手段使电子档案管理的安全性和可靠性性得到进一步提升。

5.5 企业办公终端数据安全使用场景

参考适用场景：企业办公终端上数据安全使用场景

表 5 企业办公终端数据安全使用场景典型威胁情境

主体	路径与客体	意图与结果
非特定主体	通过控制办公终端，利用办公终端上存储的敏感数据，进行数据买卖或者进一步窃取组织内部数据资源	恶意或非恶意泄露或公开或窃取数据

5.5.1 概要

办公终端是企业员工最重要办公设备。特别地，随着云终端、移动终端、智能终端、虚拟终端等不断推出，企业面临着各式各样多场景下，具有“合法权限”的终端接入企业内部网络和业务系统，同时，办公终端上会驻留的访问权限、历史数据和操作痕迹等。故，整个数据安全边界被打破，由于设备遗失、失窃以及

被黑客控制，最终恶意分子以终端为跳板，直接或间接获取终端、文件服务器、数据库和应用系统中的数据，导致数据安全事件频发。

5.5.2 安全现状

5.5.2.1 已完成安全建设

传统的，企业通过部署移动终端安全管理系统，辅以安全管理流程（人工审核），对访问网络、应用以及数据的办公终端，进行 IP、MAC 进行白名单管理，并进行重大风险安全补丁检测，以实现多维度管控。更多，针对第三方接入或重点区域，企业已经实施视频监控、应用系统明水印以及登录风险警告，以达到警示和威慑作用。

随着，零信任的应用，对于办公终端安全访问网络和应用，以了极好的支撑。通过部署零信任可以让用户、设备、连接对整个资源访具备主动管理的能力，实现了最小权限访问的集中管理、实时用户风险行为检测，并为整个企业网络安全态势管理提供支持。

5.5.2.2 缺失安全手段

不管是终端管控系统，还是零信任部署，抑或终端防病毒软件，对于企业数据安全保护工作来说，不具备数据级的防护，同时，终端管理和零信任需要配置较多的管理工作（百人级组织或企业，需要配置 2 名以上的专职管理人员落实日常工作）。同时，在简化用户操作，提升用户工作效率的同时，实际上会产生大量的访问日志和安全日志，需要开展海量的安全审计工作，以不断调整安全策略和识别第三方人员的资源访问、违规访问、数据操作。更多的，办终端在失控后（被窃、被遗失、被不当回收等），数据安全性极需得到保证。

办公终端中需要紧急并优先解决如下重点数据安全使用风险：

1. 办公终端未部署针对数据保护的管控手段，传统的网络接入型的终端管控手段，仅能保护内部资源。但是终端中缓存的数据，以及访问权限极有可能导致访问权限失控；

2. 办公终端中大量敏感数据，如配置文件、缓存口令、电子邮件、移动办公 OA 中的数据都有可能在设备失控时，对企业的数据保护造成破坏。

5.5.3 增强方案

建议企业管理者单位结合 DTTACK 模型，在传统网络安全和零信任部署的基础上，进行如下方案分析与设计：

需求一实现：选择 4.2 P:防护^4.2.7 技术：DLP 技术^4.2.7.1 扩展技术：终端 DLP 技术；选择 4.2 P:防护^4.2.7 技术：DLP 技术^4.2.7.4 扩展技术：邮件 DLP 技术；选择 4.6 C:反制^4.6.1 技术：水印技术^4.6.1.2 扩展技术：多媒体水印技术；

需求二实现：选择 4.2 P:防护^4.2.1 技术：数据加密技术^4.2.1.1 扩展技术：存储加密^# FDE 全磁盘加密方法；选择 4.2 战术：防护^4.2.9 技术：云数据保护技术^4.2.9.1 扩展技术：云密码服务^# 密钥管理；

需求三实现：选择 4.6 C:反制^4.6.1 技术：水印技术^4.6.1.4 扩展技术：屏幕水印技术；选择 4.2 P:防护^4.2.5 技术：访问控制^4.2.5.4 扩展技术：数据访问控制技术。

整体安全增强设计如下图所示：

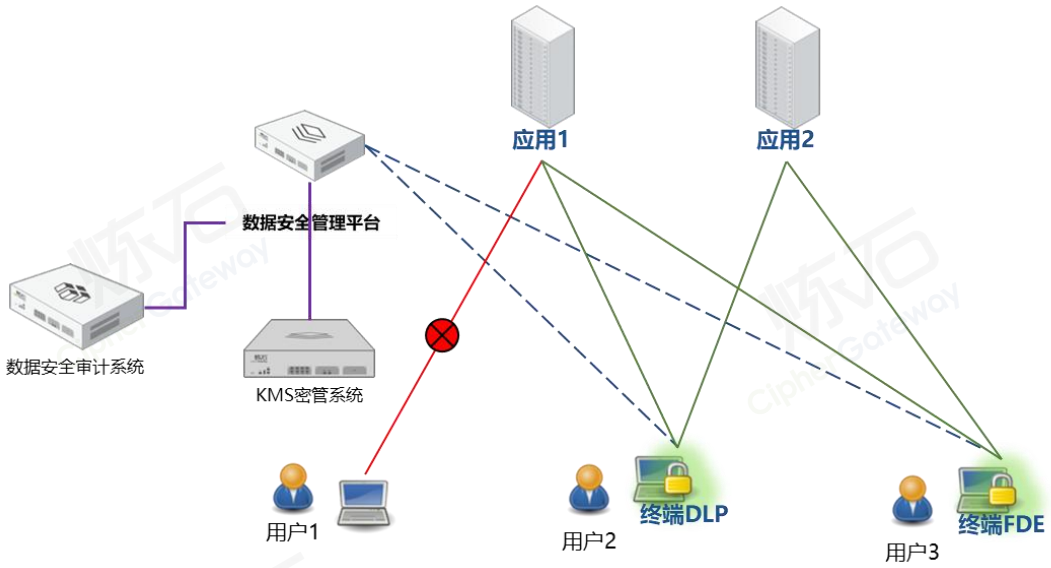

图 25 终端数据保护实现示意图

5.5.4 总结

通过建设终端 DLP 和终端 FDE 数据安全保护棲，设置安全防护策略，对终端上所有敏感文件实现 SM4 加密，对终端上数据访问行为，操作行为进行安全监测，结合传统终端管控系统以及零信任，及时分析风险分析和记录违规事件，，并实现用户终端设备失控后敏感数据安全保护。

5.6 政务大数据交换共享场景

参考适用场景：政务类平台的数据存储、数据提供场景

表 6 政务大数据交换共享场景典型威胁情境

主体	路径与客体	意图与结果
内部工作人员	录入数据	非故意注入恶意代码、不良信息

第三方人员或内部技术人员或黑客	维护数据库;非法访问数据库	滥用权限或恶意攻击,获取原始敏感数据
合作方或黑客	非法接口请求或滥用接口	非法利用交换共享接口实施“拖库”或“撞库”等攻击

5.6.1 概要

电子政务公共数据开放共享平台项目建设目标是，依托统一的“云”数据中心建设统一的公共数据开放共享平台。集中机关各部门业务应用进行，制定相关的数据规范和信息交换标准,使机关各部门业务系统依托统一的开放平台进行开发建设。确保部门之间系统之间的互联互通、数据共享，为大数据分析提供数据依据。

5.6.2 安全现状

5.6.2.1 已完成安全建设

结合相关国家标准和建设规范，各接入部门到电子政务公共数据开放共享平台的数据进行 VPN 加密传输。接入部门和平台两端防火墙插卡设备之间采用 IPSecVPN 协议，保证数据在传输过程中的端到端安全性。平台业务系统在传递消息的过程中可以指定采用消息内容的校验。对安全性要求比较高的业务系统来说，在调用平台的 WebService 接口时使用 HTTPS 协议，保证了传输层面的安全。平台部署了数据库审计产品来实现对数据安全审计及防护。

5.6.2.2 缺失安全手段

在多年运营情况来分析，由于平台规划设计阶段未充分考虑收集数据数量和速率呈现倍数增长引发新安全隐患，未充分考虑数据对外共享接口管理可能出现失控，面临数据安全、个人信息保护方面新法规要求，导致平台持续健康运营存在安全风险。综合分析，平台需要紧急解决如下场景化数据安全问题：

1. 从各委办局录入或采集数据需要实现内容合规、数据安全（文档、数据库），同时要平衡人工审核和智能化投入成本；

2. 数据库存储的数据包含个人信息（含敏感信息）、公共数据（含重要数据），要实现数据库字段的数据加密存储，减少内部技术人员和黑客获取原始敏感数据的风险，同时符合多品牌、多版本数据库现状；

3. 对外共享数据时，需要防止接口调用方滥用接口，或者攻击接口（非法请求），利用共享接口发起“拖库”或“撞库”等攻击。

5.6.3 增强方案

建议平台管理者单位结合 DTTACK 模型，进行如下方案分析与设计：

需求一实现：选择 4.1 I:识别^4.1.3 技术：数据资产处理（分析）^4.1.3.1 扩展技术：数据内容识别与 4.1.5.1 扩展技术：标记字段法技术；选择 4.3 D:检测^4.3.2 技术：流量监测^4.3.2.1 扩展技术：网络流量分析；4.3.2.2 扩展技术：高级安全分析技术；针对电子政务类数据类型，筛选并建立行业敏感字段、数据库字段等特征库；利用识别算法和检测算法实现持续优化；

需求二实现：选择 4.2 P:防护^4.2.1 技术：数据加密技术^4.2.1.1 扩展技术：存储加密^# 应用内加密（AOE 面向切面加密）方法与 4.2.2 技术：数据脱敏技术

^4.2.2.2 扩展技术：静态脱敏技术；针对电子政务类数据类型，筛选并建立行业敏感字段（主要参考《政府数据 数据分类分级指南》、DB44 2110-2018《电子政务数据资源开放数据技术规范》、DB52-T1123-2016《政府数据数据分类分级指南》等）、数据库字段等特征库；利用加密模块实现敏感字段字段级加密；

需求三实现：选择 4.1 I:识别^4.1.1 技术：数据资源发现^4.1.1.2 扩展技术：应用接口探测技术；选择 4.3 D:检测^4.3.5 技术：共享监控^4.3.5.3 扩展技术：接口访问预警技术;利用接口资产管理模块和管控模块,实现接口数据传输速率、数据包大小、异常访问行为等检测。

整体安全增强设计如下图所示：

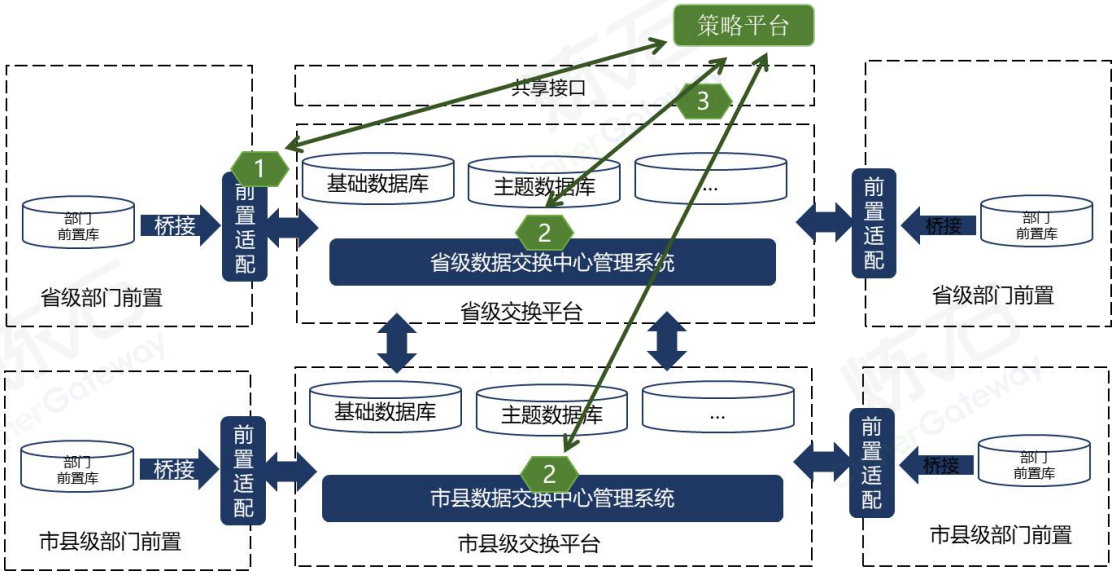

图 26 简要政务大数据交换共享平台安全增强设计示意

在增强点 1，在前置适配服务器上部署多版本支持的检测模块（软件模块），实现文档内容合规扫描，列数据安全扫描，恶意程序检测等。

在增强点 2，在管理系统中部署 AOE 加密模块（软件模块），解析业务 SQL，数据库入库前即加密，实现字段级密文存储。

在增强点 3，在接口服务器上部署接口安全管控模块，实施接口非法调用，接口异常访问，接口传输管控等。

增强点上实现软部署，所有软模块由策略平台统一管理或驱动。

5.6.4 总结

随着法律法规监管日趋收紧，前期缺乏数据安全顶层设计的政务大数据交换共享平台面临数字经济发展和数据安全双重挑战。在尽量不改动平台架构与设计的前提下，重点考虑平台业务特性，贴合平台业务形态设计专有数据安全方案变得必要。参考 DTTACK 模型，从数据安全保护角度，查漏补缺，实现平台数据安全防护能力快速迭代，解决痛点问题，并最大化降低不必要或非紧急安全投入，平衡合规、威胁和安全投入。

5.7 银行业数据安全增强方案

参考适用场景：银行业敏感数据安全存储场景

表 7 银行业敏感数据安全存储场景典型威胁情境

主体	路径与客体	意图与结果
第三方人员或内部技术人员或黑客	维护文件服务；非法访问文件服务器	滥用权限或恶意攻击，获取原始敏感数据
内部业务人员等、第三方合作单	数据对外提供和共享时无控制手	恶意访问并泄露或公开敏感数据

位	段	
非特定主体	通过控制办公终端，利用办公终端上存储的敏感数据，进行数据买卖或者进一步窃取组织内部数据资源	恶意或非恶意泄露或公开或窃取数据

5.7.1 概要

银行业的数字化转型意味着大量数据的快速积累，因其强大的业务渗透性，数据已成为当下机构组织的核心资产。随之而来，在其生产、传输、存储、使用和处理的过程中，银行业及关联行业面临着空前的安全风险的严峻挑战。在数据泄露类型中，个人数据信息排首位，其次是凭证和银行数据。Verizon 2021 数据泄露调查报告显示，今年，金融服务领域 44% 的违规行为是由内部参与者造成的，占当年所有违规的 13%。而其中，多数人员的行为属于偶然，特别是误发电子邮件的人员事件，占全年所有误发电子邮件违规事件的 55%。

5.7.2 安全现状

5.7.2.1 已完成安全建设

近年来，国家各个部门推出的监管要求，对银行的信息领域提出明确要求，银行在发展中首要解决来自监管层的合规刚需，达到法规要求：《网络安全法》《数据安全法》《信息安全等级保护》《等保 2.0》《银行业金融机构数据治理指引》《个人信息保护法》等。

其次，银行的稳定可持续发展，亟待大幅度完善内部信息化管理机制和提高

自身数据信息的治理能力，用于防护、规避各类隐患，谨慎面对业务中诸如网络渗透威胁、数据库运维安全、软件开发测试环境数据脱敏、终端敏感数据泄露、邮件/网络敏感数据泄露、移动办公数据泄露、内部人员的违规访问、数据底账不清、安全审计追溯定责等安全风险。

5.7.2.2 缺失安全手段

安全风险：

1、内部核心人员为了个人利益恶意泄露核心数据

内部高层核心人员为了争取个人利益，选择违规或越权访问核心数据，将核心数据发送给第三方单位从中获利，严重违背职业道德甚至是法律制度。这类人群在银行内部本身就拥有较高级别的数据管理权限和信任基础，工作之便易于接触核心数据信息，一旦发生恶意泄露事件，损失往往不可估量。

2、内部职员办公网络环境缺乏防护，无意泄露数据

由于病毒木马的泛滥以及企业员工自身对于电脑设备的网络安全防范意识的缺乏，使得企业数据泄密的风险越来越大。内部邮件系统或办公电脑一旦遭到入侵，大量数据资料也将同步被流失。不管投入多少，有些职员永远不会对安全意识培训做出反应，而这些人多数会成为网络钓鱼诈骗的反复受害者。

3、远程办公导致数据泄露，文件存储设备的损坏维修或丢失

远程办公人员不可避免地使用移动存储设备。例如笔记本电脑、移动硬盘、手机存储卡、数码照相/摄录机等，没有统一的设备管理、排查和防护制度，一旦遗失、维修或报废，存储数据暴露无遗。这也是泄密事件发生的主因之一。

IBM 报告显示：2021 年数据泄露成本增长了近 10%，创下历史新高。由于疫情大流行导致的远程工作导致数据泄露的成本迅速上升，在超过 50%的组织中，平均需要 316 天才能识别并控制违规行为。而平均情况是 287 天，远程工作使控制数据泄露的时间延长了一个月。

5.7.3 增强方案

建议银行管理者结合 DTTACK 模型，进行如下方案分析与设计：围绕客户数据、内部核心信息、知识财产及敏感或机密信息等进行精细化数据管理，实现了资产价值的最大化：

需求一实现：选择 4.2 P:防护^4.2.5 技术：访问控制^4.2.5.4 扩展技术：数据访问控制技术，采用权限管理为核心，结合加解密技术，实现对受控文档的精确权限控制，有效控制使用者对核心数据文档的阅读、修改、打印、授权、解密等操作权限，从根源上防止文档在使用者之间非法使用而导致核心数据泄露。通过数据库安全审计系统，对数据库操作行为进行监控，为事后追溯定责提供准确依据，同时对风险行为配备实时报警系统；

需求二实现：选择 4.2 P:防护^4.2.2 技术：数据脱敏技术，对敏感数据进行变形、屏蔽、替换、随机化、加密，将敏感数据转化为脱敏数据。选择 4.2 P:防护^4.2.7 技术：DLP 技术，终端、网络、邮件数据防泄漏可以确保重要信息避免通过 USB/CD/DVD 或 IM 类聊天工具、Internet 协议、SMTP 邮件、WEB 邮件等离开可控范围；

需求三实现：选择 4.2 P:防护^4.2.2 技术：数据脱敏技术技术，以 AOE\TFE 和 ABAC 权限管理等技术为支撑，对数据及文件实时加密，集成动态加密、身份

识别认证等技术，在不影响工作习惯及业务效率的前提下，有效防止数据泄露。

5.7.4 总结

在遵循《网络安全法》《数据安全法》《信息安全等级保护》《等保 2.0》《个人信息保护法》等的合规要求下，银行业需要在数据的存储态、使用态、传输态进行安全防护，防止数据泄露，建立以数据加解密为核心的防控机制，结合权限管控及虚拟化技术保障核心数据内部及外发使用安全。现时，可考虑建立安全管控可视化平台，以统一策略为基础，采用深度内容识别技术对静态数据、动态数据及使用中的数据进行识别、管控、审计，形成可视化地呈现敏感数据分布状况和安全态势帮助用户进行补救以及追溯操作。

5.8 互联网金融数据安全使用场景

参考适用场景：互联网金融领域数据使用、共享场景

表 8 互联网金融数据安全使用场景典型威胁情境

主体	路径与客体	意图与结果
内部业务人员、黑客	利用访问控制暗点和安全审计时差，非法访问数据	恶意窃取数据
内部业务人员等、第三方合作单位	数据对外提供和共享时无控制手段	恶意访问并泄露或公开敏感数据
黑客或应用程序、数据	运维应用或设备，非授权	恶意窃取数据

库、主机、存储运营人员	访问敏感数据	

5.8.1 概要

习近平总书记指出，金融是国家重要的核心竞争力，金融安全是国家安全的重要组成部分。可以说，金融是国家重要的核心竞争力，是现代经济的核心。对于金融行业，数据逐步转变为核心价值资产。但是，随着互联网新技术在金融行业的广泛应用和融合，互联网金融业务多数采用网络与应用高负载和高并发，兼容高速缓存的微服务类的金融电子商务平台架构。同时,个人信息是互联网金融业务重要运营资源。

5.8.2 安全现状

5.8.2.1 已完成安全建设

相比于传统的金融业务，互联网金融系统架构具备较完备网络安全顶层设计，完善的风控管理体系以及交易、支付风险管理。绝大多数互联网金融平台会设计环节开展等级保护建设，定期开展风险评估并部署实时威胁检测系统。

较其它经济领域，互联网金融领域的行业监管和指导更加严苛。多数企业组建了专职网络安全管理团队，并明确岗位职责。

在安全技术防护手段层面，互联网金融企业在等级保护相关要求指导下，结合行业龙头经验，实现较完整网络安全防护，如 DDoS 攻击防护、Web 应用防护、系统安全、态势感知、SSL 证书等。

5.8.2.2 缺失安全手段

网络安全合规和金融风控要求帮助互联网金融企业完成了安全基本面的建设；但是，数据黑产一直互联网金融企业安全痛点，与此同时《密码法》、《数

据安全法》、《个人信息保护法》的相关法律的陆续正式实施，由数据保护失位产生的惩罚性罚款和法律风险成为互联网金融领域相关企业的达摩克利斯之剑。

互联网金融企业需要建立一整套完整的数据安全治理体系，在数据的收集、存储、使用、加工、传输、提供、公开等各个处理环节，施加完善的安全策略、人员责任、安全作业等治理手段，并部署相关的数据安全产品。但是，考虑到投入资金、精力、时间，互联网金融企业更加需要考虑通过高效的数据安全技术手段解决在业务快速迭代背景下显著性数据安全风险。

互联网金融行业需要紧急并优先解决如下重点数据安全使用风险：

1. 内部人员滥用数据或内外部勾结滥用和窃取数据的行为，防止数据泄露；

2. 数据对外提供和共享时，被滥用，且缺乏抗抵赖手段造成追责困难或承担连带责任；

3. 内部人员访问及使用数据时，访问控制手段过于粗放，导致安全威慑力不够和追责困难。

5.8.3 解决方案

建议互联网金融企业管理者单位结合 DTTACK 模型，对企业数据安全治理进行如下技术方案分析与设计：

需求一实现：选择 4.2 P:防护^4.2.1 技术：数据加密技术^4.2.1.1 扩展技术：存储加密^# 应用内加密（AOE 面向切面加密）；选择 4.2 P:防护^4.2.9 技术：云数据保护技术^4.2.9.1 扩展技术：云密码服务^# 密钥管理；选择 4.2 P:防护^4.2.1 技术：数据加密技术^4.2.1.1 扩展技术：存储加密^# TFE 透明文件加密方法；

需求二实现：选择 4.1 I:识别^4.1.4 技术：数据分类分级^4.1.4.1 扩展技术：自动化工具^# 自动化数据分类分级打标技术；选择 4.7 G:治理^4.7.4 数据安全管理^4.7.4.1 数据安全评估技术；选择 4.6 C:反制^4.6.1 技术：水印技术^4.6.1.2 扩展技术：多媒体水印技术；选择 4.7 G:治理^4.7.7 数字道德^# AvanadeTrendlines：数字道德技术；

需求三实现：选择 4.2 P:防护^4.2.5 技术：访问控制^4.2.5.2 扩展技术：权限管理控制^# ABAC 技术。

5.8.4 总结

利用 DTTACK 模型，选择适宜的技术方案，规避互联网金融业务面临的重要数据安全风险。进而结合数据安全治理和个人隐私保护要点，健全数据治理体系，遵循《数据安全法》、《个人信息保护法》等数据安全的有关法律法规标准规范，建立数据安全保护体系，防止重要数据和个人信息被泄露、篡改和滥用。

同时，方案可以很好支撑公安部《信息安全等级保护》、《金融行业网络安全等级保护实施指引》、《金融行业网络安全等级保护测评指南》以及《网络安全法》、《密码法》的等法律法规的要求。

5.9 民航业数据安全存储场景

参考适用场景：民航业敏感数据安全存储场景

表 9 民航业敏感数据安全存储场景典型威胁情境

主体	路径与客体	意图与结果
第三方人员或内部技术	维护文件服务；非法访问	滥用权限或恶意攻击，获

人员或黑客	文件服务器	取原始敏感数据
非特定主体	落实数据安全合规管理要求	落实数据安全合规管理要求

5.9.1 概要

航空公司的应用系统中拥有大量旅客和员工的个人信息数据,涉及敏感信息的业务系统，包含售票、安检、值机、通关、登机、离港、行李托运、贵宾室、旅客核心库等系统；加密字段内容包括公民个人身份信息，包括姓名、手机号、身份证号、邮箱等结构化数据；以及个人身份证照片、人脸图像等非结构化数据。

航空公司的业务是围绕旅客展开的,旅客个人隐私数据的安全关系着企业的声誉和利益，如何在促进数据共享、发挥数据价值的同时保障数据安全是需要重点解决的问题。同时，受国外 GDPR 及国内《网络安全法》、《密码法》、《数据安全法》及《个人信息保护法》等法律法规的合规要求，需建设数据安全密码防护平台，采用密码技术来保护个人信息及企业敏感数据的安全。

针对航空公司信息系统数量众多、逻辑关联复杂、数据高速流转的特点，需要一套完整严密的数据安全体系来保障数据安全，即直接作用于敏感数据，易于部署，对应用免开发改造的数据安全技术，才能符合航空公司业务实际需要，才能真正发挥作用。

5.9.2 安全现状

5.9.2.1 已完成安全建设

航空公司多年历史的沉淀，已经具备相当比较完善的网络安全保护措施：

（1）设置登录设备及系统的身份认证及用户权限；

（2）防火墙和入侵检测系统。定期进行系统及数据库进行安全检测。防止对系统和数据库的外部攻击，并规避内部运维带来的风险；

（3）IPSEC/SSL VPN 保障网络间及客户端和服务端间的安全传输通道；

（4）系统与数据的备份；

（5）安全审计系统。对业务人员及运维人员操作进行细粒度的审批和管控；对风险操作进行实时告警，监控系统和数据库的运行状况。

5.9.2.2 缺失安全手段

尽管航空公司针对系统网络安全及数据安全已做了诸多的防护措施，仍然有数据泄露事件的发生，归根结底是由于数据库里存储的数据是明文数据。

民航公司需要解决如下数据安全风险：

（1）防止外部窃取：防止由于黑客攻击 数据库和应用造成的数据泄露；

（2）防止内部数据泄露：防止数据使用过程中的敏感数据滥用造成的数据泄露；

（3）满足合规需求：满足国家法律、法规及民航行业数据安全管理规定。

5.9.3 解决方案

建议管理者结合 DTTACK 模型，进行如下方案分析与设计：

需求一实现：选择 4.2 P:防护^4.2.1 技术：数据加密技术^4.2.1.1 扩展技术：存储加密^# 应用内加密（AOE 面向切面加密）方法；针对民航数据类型，筛选

并建立行业敏感字段、数据库字段等特征库；利用脱敏模块实现敏感字段字段级加密；

需求二实现：选择 4.2 P:防护^4.2.1 技术：数据加密技术^4.2.1.1 扩展技术：存储加密^# 应用内加密（AOE 面向切面加密）方法；

具体地，通过建立数据加解密平台，包含密钥管理系统、数据安全平台及加解密插件。平台提供了“集中式管理、分布式加密”的模式，为航空公司各个信息系统提供加解密及脱敏服务，只需在目标应用中配置数据加解密插件，插件中包含高性能国密中间件，即可实现以下数据安全防护目标：

实现免开发改造应用系统，实现增强业务应用的数据安全能力的同时，而不影响现有业务系统的稳定性，保证已上线系统的正常运营、不中断。实现进入数据库的结构化敏感数据的加密，防止数据库被拖库。实现对于非结构化文件类数据的加密保护。

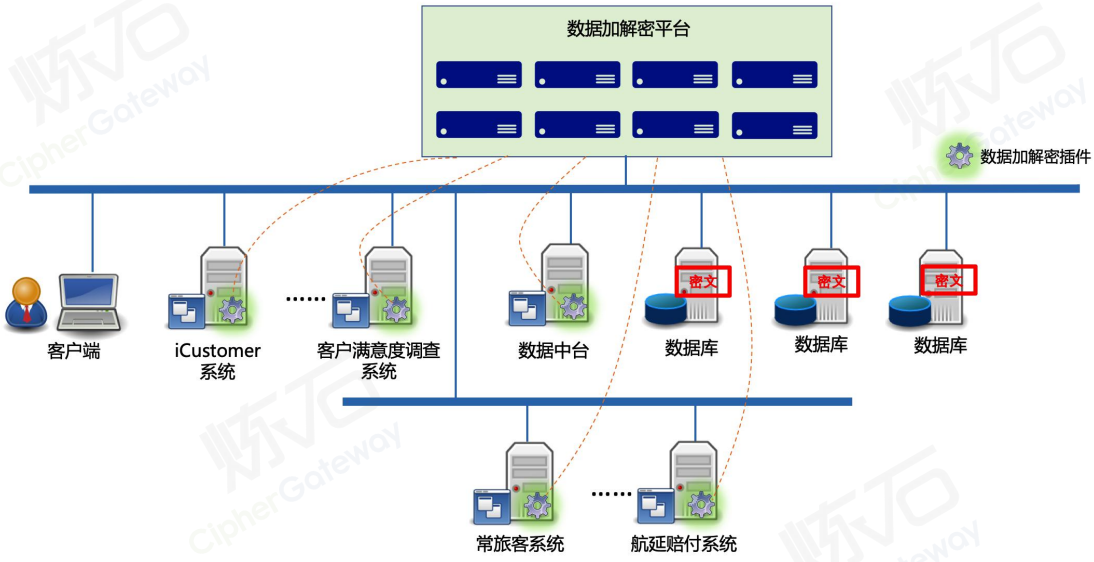

图 27 数据加解密平台总体框架图

5.9.4 总结

数据加解密平台的建设，为航空公司初步建立起以密码技术为核心的实战化数据安全密码防护体系。采用创新 SM4 等国密技术，符合国家信息系统密码应用安全及安全性评估的合规要求。且支持免改造应用系统的模式实现数据加密，能够有效保护旅客个人隐私数据(包括存储于数据库中个人敏感信息的结构化数据，及存储于文件服务器磁盘中的个人照片等非结构化数据)，从而应对航空交通业务发展中的数据安全挑战，助力保护旅客的重要敏感信息免于遭受威胁，有力保障了重要数据的安全，降低数据泄露风险，使得业务安全有序开展。

5.10 电力数据中台的数据安全增强

参考适用场景：电力数据中台的数据安全增强方案

表 10 电力数据中台的数据安全增强典型威胁情境

主体	路径与客体	意图与结果
第三方人员或内部技术人员或黑客	维护文件服务;非法访问文件服务器	滥用权限或恶意攻击，获取原始敏感数据
非特定主体	落实数据安全合规管理要求	落实数据安全合规管理要求

5.10.1 概要

目前电力企业正处在数字化转型期，数据资产已上升到战略资源层面，对数据安全管理提出了更高的要求。结合目前国家信息安全形势，电力企业越来越重

视信息系统安全防护，对电力核心业务进行数据安全保护，保障核心业务数据即使被非法用户获取后，也无法提取出有用信息，是电力数据中台安全防护的关键。

5.10.2 安全现状

5.10.2.1 已完成安全建设

1. 通过防火墙过滤、访问控制、动态身份验证系统、防 DoS 攻击，提高对非法数据、病毒攻击的防护。

2. 通过 MPLS VPN 的部署，对各个 VPN 之间提供逻辑隔离功能，有效地防止 VPN 之间的攻击行为。

3. 部署 NIDS 系统，对网络中各种行为、应用服务实时监控，提前预警潜在的安全风险。

5.10.2.2 缺失安全手段

基于省市公司对集中存储数据的使用存在安全顾虑和规避信息系统外部审计工作中的风险和安全形势及公司信息系统安全防护的需求，需迫切开展适应数据中台架构的数据安全分级研究，设计各级企业内数据的安全分级和使用策略，为数据的安全使用和维护提供指导，降低数据丢失、泄露的风险，保护企业数据安全。

具体的措施是以下三方面：

1. 依据数据重要性、敏感性进行安全分级，对分级后的数据采取相应该等级的保护措施。

2. 对分级后的数据进行分级存储，对敏感数据进行加密存储。

5.10.3 解决方案

建议电力企业管理者结合 DTTACK 模型，进行如下方案分析与设计：

需求一实现：选择 4.3 D:检测^4.3.5 技术：共享监控^4.3.5.3 扩展技术：接口访问预警^# 文字识别 技术；选择# 图片识别技术；

需求二实现：选择 4.2 P:防护^4.2.1 技术：数据加密技术^4.2.1.1 扩展技术：存储加密^# 应用内加密（AOE 面向切面加密）方法；针对电力数据类型，筛选并建立行业敏感字段、数据库字段等特征库；利用脱敏模块实现敏感字段字段级加密。选择# 应用内加密（AOE 面向切面加密）方法；

具体地，根据应用、数据等访问客体属性，包括分级、分类、资源、功能等因素，对访问客体进行分级管理防护。访问主体与客体是严格隔离的，访问主体不可直接访问客体资源。针对主体访问客体的信息流，基于访问主体的属性和操作，访问客体的属性以及授权策略，制定精细化的授权访问策略模型，形成主体、客体和环境属性实现动态映射机制。基于智能身份分析进行风险评估和环境感知，实现动态访问控制，提供灵活的权限管理，对用户和设备权限进行动态过滤与裁剪，消除权限过大风险。

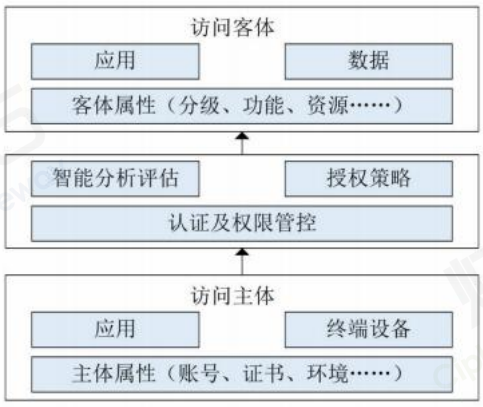

图 28 数据中台“零信任”安全防护架构

数据等级	保护场景	数据识别	保护技术措施	数据安全监视
三、四级（机密性高）	能够保护的对象：从数据域里下载或导出到桌面终端进行应用的数据文件（如 word 文件、pdf 文件、数据表文件等），相应的等需在数据文件进行标识	数据保护中的文件检索，通过检索数据文件的标识发现数据等级，并采取相应的保护措施	数据文件加密、屏幕水印、通过数据文件指纹信息最终数据文件流转过程、操作行为审计（对文件的拷贝、移动、增删改查、外发、拷贝、打印、传输等）	通过数据保护管理子系统可监视数据文件在终端上的具体分布情况、数据全生命周期监视、数据文件的合规分析
二级（机密性中）	能够保护的对象：从数据域里下载或导出到桌面终端进行应用的数据文件（如 word 文件、pdf 文件、数据表文件等），相应的等级需在数据文件进行标识	数据保护中的文件检索，通过检索数据文件的标识发现数据等级，并采取相应的保护措施	数据文件加密，屏幕水印、对数据文件的危险操作进行审计（比如：外发、U 盘拷贝、打印、不明网络传输等）	通过数据保护管理子系统可监视数据文件在终端上的具体分布情况、数据文件的合规分析
一级（机密性低）	能够保护的对象：从数据域里下载或导出到桌面终端进行应用的数据文件（如 word 文件、pdf 文件、数据表文件等），相应的等级需在数据文件进行标识	数据保护中的文件检索，通过检索数据文件的标识发现数据等级，并采取相应的保护措施	数据文件加密	通过数据保护管理子系统可监视数据文件在终端上的具体分布情况

图 29 等级保护说明图

1. 数据中台应用租户创建与配置：根据数据分级分类规范，创建不同级别的应用用户，分别用于存储不同级别数据，基于数据中台租户模式实现各级数据隔离以及数据访问权限控制。

2. 利用数据中台数据传输功能，按照数据分级分类规范，使用不同应用用户完成数据接入至数据中台数据仓库，实现数据分级存储和管理。

3. 应用内集成加密 SDK，对数据进行加密，在完成数据加密后，通过数据传输组件接入至数据中台。

5.10.4 总结

针对当前电力数据中台安全防护的需要，提出了基于数据中台的数据安全分级防护方案，给出了数据中台“零信任”安全防护总体架构，阐述数据分级方法和定级标准，设计了差异化的数据安全保护策略，验证了基于数据中台的数据安全分级防护方案的可行性和有效性。

附录：数据安全相关法律政策、技术标准汇总

表 11 数据安全与个人信息保护相关合规政策列举

时间/国标号	名称	条例
顶层规划		
2020 年 3 月 30 日	中共中央国务院关于构建更加完善的要素市场化配置体制机制的意见	坚持安全可控，加强数据资源整合和安全保护
2021 年 3 月 5 日	2021 年政府工作报告	加强网络安全、数据安全和个人信息保护
2021 年 3 月 11 日	中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要	加快推进数据安全、个人信息保护等领域基础性立法，强化数据资源全生命周期安全保护。
法律法规		
2015 年 7 月 1 日起施行	中华人民共和国国家安全法	第二十五条 国家建设网络与信息安全保障体系，提升网络与信息安全保护能力，加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领域信息系统

		及数据的安全可控；加强网络管理，防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为，维护国家网络空间主权、安全和发展利益。
2017 年 6 月 1 日起施行	中华人民共和国网络安全法	第十八条：国家鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展。
2020 年 1 月 1 日起施行	中华人民共和国密码法	第二十七条：法律、行政法规和国家有关规定要求**使用商用密码进行保护的关键信息基础设施，**其运营者应当使用商用密码进行保护。关键信息基础设施运营者，**应当自行或者委托商用密码检测机构开展商用密码应用安全性评估。**
2021 年 1 月 1 日起施行	中华人民共和国民法典	第一百一十一条 自然人的个人信息受法律保护。任何组织或者个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。 第一千零三十八条 信息处理者不得泄露或者篡改其收集、存储的个人信息；未经自然人同意，不得向他人非法提供其个人信息，但是经过加工无法识别特定个人且不能复原的除外。 信息处理者应当采取技术措施和其他必要措施，确保其收集、

		存储的个人信息安全，防止信息泄露、篡改、丢失；发生或者可能发生个人信息泄露、篡改、丢失的，应当及时采取补救措施，按照规定告知自然人并向有关主管部门报告。
2021 年 9 月 1 日起施行	中华人民共和国数据安全法	第十九条：国家根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者公民、组织合法权益造成的危害程度，对数据实行分级分类保护。 第二十五条：**采取相应的技术措施和其他必要措施**，保障数据安全。
2021 年 11 月 1 日起施行	中华人民共和国个人信息保护法	第五十一条第二款：对个人信息实行分类管理；第三款：采取相应的加密、去标识化等安全技术措施； 第六十六条：情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处**五千万元以下或者上一年度营业额百分之五**以下罚款……
政策制度		
2017 年 4 月 11 日	个人信息和重要数据出境安全评估办法（征求意见	第三条 数据出境安全评估应遵循公正、客观、有效的原则，保

	稿）	障个人信息和重要数据安全，促进网络信息依法有序自由流动。
2018 年 6 月 27 日	网络安全等级保护条例（征求意见稿）	第六条：保障网络基础设施安全、网络运行安全、数据安全和信息安全； 第四十九条：对第三级以上网络运营者按照网络安全等级保护制度落实网络基础设施安全、网络运行安全和数据安全保护责任义务，实行重点监督管理。
2019 年 5 月	数据安全管理办法（征求意见稿）	第三条 国家坚持保障数据安全与发展并重，鼓励研发数据安全保护技术。第六条制定数据安全计划，实施数据安全技术防护，开展数据安全风险评估。
2020 年 2 月 1 日起施行	国务院办公厅关于印发国家政务信息化项目建设管理办法的通知（国办发〔2019〕57 号）	第四章第三十条：各部门应当严格遵守有关保密等法律法规规定，构建全方位、多层次、一致性的防护体系，按要求采用密码技术，并定期开展密码应用安全性评估，**确保政务信息系统运行安全和政务信息资源共享交换的数据安全。**
2020 年 6 月 1 日	网络安全审查办法	第三条 网络安全审查坚**持防范网络安全风险与促进先进技术应用相结合**、过程公正透明与知识产权保护相结合、事前审查与持续监管相结合、企业承诺与社会监督相结合，从产品和服

		务安全性、可能带来的国家安全风险等方面进行审查。 第五条 运营者采购网络产品和服务的,应当预判该产品和服务投入使用后可能带来的国家安全风险。影响或者可能影响国家安全的，应当向网络安全审查办公室申报网络安全审查。
2020 年 7 月 22 日	贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见（公网安〔2020]1960 号）	第一部分第一点：以保护关键信息基础设施、重要网络和**数据安全**为重点；第三点：关键信息基础设施涉及的关键岗位人员管理、供应链安全、**数据安全**、应急处置等重点安全保护措施得到落实。 第三部分第四点：加强重要数据和个人信息保护。运营者应建立并落实重要数据和个人信息安全保护制度，对关键信息基础设施中的重要网络和数据库进行容灾备份，采取**身份鉴别、访问控制、密码保护、安全审计、安全隔离、可信验证等关键技术措施，**切实保护重要数据全生命周期安全。
2020 年 8 月 20 日	商用密码管理条例（修订草案征求意见稿）	第三十五条 国家鼓励公民、法人和其他组织依法使用商用密码保护网络与信息安全，鼓励使用经检测认证合格的商用密码。 第三十八条 非涉密的关键信息基础设施、网络安全等级保护第三级以上网络、国家政务信息系统等网络与信息系统，其运营

		者应当使用商用密码进行保护，制定商用密码应用方案，配备必要的资金和专业人员，同步规划、同步建设、同步运行商用密码保障系统，自行或者委托商用密码检测机构开展商用密码应用安全性评估。
2020 年 9 月	全球数据安全倡议	各国承诺采取措施防范、制止利用网络侵害个人信息的行为，反对滥用信息技术从事针对他国的大规模监控、非法采集他国公民个人信息。
2021 年 9 月 1 日起施行	关键信息基础设施安全保护条例	第十五条第六点：履行**个人信息和数据安全**保护责任，建立健全**个人信息和数据安全**保护制度。
–	数据安全管理条例	2021 年 5 月 27 日，《数据安全管理条例》纳入国务院 2021 年度立法工作计划。
技术标准		
基础定义		
GM/Z0001-2013	密码术语	给出商用密码工程领域的基础术语及定义
GB/T 25069-2010	信息安全技术 术语	界定了与信息安全技术领域相关的概念的术语和定义，并明确

		了这些条目之间的关系。
重要数据安全规范标准		
工信部	电信和互联网行业数据安全标准体系建设指南	发挥标准对电信和互联网行业数据安全的规范和保障作用，加快制造强国和网络强国建设步伐。
GB/T 37988-2019	信息安全技术 数据安全能力成熟度模型	给出了组织数据安全能力的成熟度模型架构，规定了数据采集安全、数据传输安全、数据存储安全、数据处理安全、数据交换安全、数据销毁安全、通用安全的成熟度等级要求。该标准适用于对组织数据安全能力进行评估，也可作为组织开展数据安全能力建设时的依据。
GB/T 35274—2017	信息安全技术 大数据服务安全能力要求	将大数据作为服务的形式，对提供者和使用者提出了安全要求。
GB/T 35282-2017	信息安全技术 电子政务移动办公系统安全技术规范	规定了电子政务移动办公系统的基本结构、安全框架，以及移动终端安全、信道安全、移动接入安全和服务端安全应满足的技术要求。
GB/T 36618-2018	信息安全技术 金融信息服务安全规范	对金融信息服务提供商的内部管理及安全技术等方面提出了基本要求，标准的制定将有利于金融信息服务提供商规范金融信息服务过程，防范金融信息服务安全风险，不断提高金融信息

		服务质量。
GB/T 39725—2020	信息安全技术 健康医疗数据安全指南	健康医疗数据控制者在保护健康医疗数据时可采取的安全措施，指导健康医疗数据控制者对健康医疗数据进行安全保护，也可供健康医疗、网络安全相关主管部门以及第三方评估机构等组织开展健康医疗数据的安全监督管理与评估等工作时参考。
GB/T 39412—2020	信息安全技术 代码安全审计规范	规定代码安全的审计过程以安全功能缺陷、代码实现安全缺陷、资源使用安全缺陷、环境安全缺陷等审计指标及对应的证实方法。
GB/T 20945—2013	信息安全技术 信息系统安全审计产品技术要求和测试评价方法	为评估信息系统的安全性和风险和完善安全策略制定提供设计数据和审计服务支撑,从而达到保障信息系统正常运营的目的。
GB/T 25061—2020	信息安全技术 XML 数字签名语法与处理规范	规定创建和表示 XML 数字签名的处理规则、签名语法和附加的签名语法，用于制作和处理 XML 数字签名的应用程序、系统或服务。
GB/T 20261—2020	信息安全技术 系统安全工程 能力成熟度模型	它关注信息技术安全（ITS）领域内的某个系统或者若干相关系统实现安全的要求。

GB/T 28458—2020	信息安全技术 网络安全漏洞标识与描述规范	规定了网络安全漏洞（以下简称“漏洞”）的标识与描述信息，适用于从事漏洞发布与管理、漏洞库建设、产品生产、研发、测评与系统运营等活动的各类组织。
GB/T 30276—2020	信息安全技术 网络安全漏洞管理规范	规定了网络安全漏洞管理流程各阶段（包括漏洞发现和报告、接收、验证、处置、发布、跟踪等）的管理要求。
GB/T 39276—2020	信息安全技术 网络产品和服务安全通用要求	规定了网络产品和服务应满足的安全通用要求，包括安全功能要求和安全保障要求。
GB/T 39680—2020	信息安全技术 服务器安全技术要求和测评准则	本标准规定了服务器的安全技术要求和测评准则，适用于服务器的研制、生产、维护和测评。
GB/T 39335—2020	信息安全技术 个人信息安全影响评估指南	规定了个人信息安全影响评估的基本概念、框架、方法和流程，适用于各类组织自行开展个人信息安全影响评估工作。同时为国家主管部门、第三方测评组织等开展个人信息安全监管、检查、评估等工作提供的指导和依据。
GB/T 39205—2020	信息安全技术 轻量级鉴别与访问控制机制	规定了轻量级的鉴别机制与访问控制机制，适用于无线传感器网络、射频识别、近场通信等资源受限的应用场景下鉴别与访问控制机制设计开发和应用。

GB/T 20283—2020	信息安全技术 保护轮廓和安全目标的产生指南	本指导性技术文件给出PP和ST文档内容的概述、示例目录清单和目标用户最关心的其他内容，并陈述了PP与ST之间的关系，以及PP和ST的开发编写过程，为使用者编写PP和ST提供指导。
–	信息安全技术 数据出境安全评估指南（征求意见稿）	规定了数据出境安全评估流程、评估要点、评估方法等内容，网络运营者按照本指南对其向境外提供的个人信息和重要数据进行安全评估，发现安全问题和风险，及时采取措施，防止个人信息未经用户同意流向境外。
–	信息安全技术 个人信息安全工程指南（征求意见稿）	描述了个人信息安全工程目标，给出了在需求分析、产品涉及、产品开发、测试审核、发布部署、运行维护等系统工程阶段的个人信息保护实施指南。
–	信息安全技术 恶意软件事件预防和处理指南(征求意见稿）	本标准给出了对恶意软件事件进行预防和处理的指南，包括恶意软件事件的预防及恶意软件事件的响应流程。
–	信息安全技术 网上购物服务数据安全指南(征求意见稿）	规定了网上购物服务可以收集、存储、使用、交换、删除、出境的数据种类、范围、方式、条件等，以及数据安全保护要求。
数据分类分级		

GB/T 30279—2020	信息安全技术 网络安全漏洞分类分级指南	本标准给出了网络安全漏洞（简称“漏洞”）的分类方式、分级指标及分级方法指南。适用于网络产品、服务的提供者、网络运营者、漏洞收录组织、漏洞应急组织在漏洞信息管理，网络产品生产、技术研发等工作。
GB/T 36632-2018	信息安全技术 公民网络电子身份标识格式规范	本标准规定了公民网络电子身份标识的组成及密钥对产生要求、格式要求和编码规则。
数据传输		
GB/T 31503-2015	信息安全技术 电子文档加密与签名消息语法	本标准规定了电子文档加密与签名消息语法,此语法可用于对任意消息内容进行数字签名、摘要、鉴别或加密。
GB/T 25061-2020	信息安全技术 XML 数字签名语法与处理规范	规定了创建和表示 XML 数字签名的处理规则、签名语法、附加的签名语法和证实方法。该标准适用于制作和处理 XML 数字签名的应用程序、系统或服务。
数据存储		
GB/T 37939-2019	信息安全技术 网络存储安全技术要求	本标准规定了网络存储的安全技术要求，包括安全功能要求、安全保障要求 。本标准适用于网络存储的设计和实现，网络存储的安全测试和管理可参照使用。

GB/T 20273-2019	信息安全技术 数据库管理系统安全技术要求	本标准是信息安全技术要求系列标准的重要组成部分，用以指导设计者如何设计和实现具有所需要的安全等级的数据库管理系统，主要从对数据库管理系统的安全保护等级进行划分的角度来说明其技术要求。
数据处理		
GB/T 37964-2019	信息安全技术 个人信息去标识化指南	描述了个人信息去标识化的目标和原则,提出了去标识化过程和管理措施。针对微数据提供具体的个人信息去标识化指导，适用于组织开展个人信息去标识化工作，也适用于网络安全相关主管部门、第三方评估机构等组织开展个人信息安全监督管理、评估等工作。
数据交换		
GB/T 37932-2019	信息安全技术 数据交易服务安全要求	规定了通过数据交易服务机构进行数据交易服务的安全要求，包括数据交易参与方、交易对象和交易过程的安全要求。
GB/T 39477-2020	信息安全技术 政务信息共享 数据安全技术要求	提出了政务信息共享数据安全要求技术框架，规定了政务信息共享过程中共享数据准备，共享数据交换、共享数据使用阶段的数据安全技术要求以及相关基础设施的安全技术要求。
数据安全管理		

GB/Z 28828-2012	信息安全技术 公共及商用服务信息系统个人信息保护指南	规范了全部或部分通过信息系统进行个人信息处理的过程，为信息系统中个人信息处理不同阶段的个人信息保护提供指导。
GB/T 35273-2020	信息安全技术 个人信息安全规范	本标准针对个人信息面临的安全问题，根据《中华人民共和国网络安全法》等相关法律，规范个人信息控制者在收集、存储、使用、共享、转让、公开披露等信息处理环节中的相关行为，旨在遏制个人信息非法收集、滥用、泄漏等乱象，最大程度地保障个人的合法权益和社会公共利益。
–	信息安全技术 个人信息工程指南（征求意见稿）	描述了个人信息安全工程目标，给出了在需求分析、产品涉及、产品开发、测试审核、发布部署、运行维护等系统工程阶段的个人信息保护实施指南。
–	信息安全技术 个人信息告知同意指南（征求意见稿）	本标准为网络运营者个人信息处理告知的内容、结构及征得个人信息主体同意收集、使用、对外提供个人信息的方式提供指导。
–	信息安全技术 移动互联网应用（APP）手机个人信息基本规范（征求意见稿）	本标准明确了移动互联网应用收集个人信息时应满足的基本要求，用以规范移动互联网应用运营者收集个人信息的行为。
安全管理体系		

GB/T 22080-2016	信息技术 安全技术 信息安全管理体系要求	本标准提供建立、实现、维护和持续改进信息安全管理体系的要求。
GB/T 22081-2016	信息技术 安全技术 信息安全控制实践指南	本标准可作为组织基于GB/T 22080实现信息安全管理体系（ISMS）过程中选择控制时的参考，或作为组织在实现通用信息安全控制时的指南。
GB/T 25067-2020	信息技术 安全技术 信息安全管理体系审核和认证机构要求	本标准的主要目的是使得认可机构在应用其评审认证机构所依据的标准时能更有效的协调一致。在GB/T 27021.1-2017和GB/T22080-2016的基础上，对实施ISMS审核和认证的机构规定了要求并提供了指南。
GB/Z 32916-2016	信息技术 安全技术 信息安全控制措施审核员指南	本指导性技术文件提供对组织信息安全控制措施进行评审的指南。例如：在组业务过程和系统环境下进行技术符合性检查等。
GB/T 28453-2012	信息安全技术 信息系统安全管理评估要求	本标准依据GB/T 20269-2006规定的信息系统分等级安全管理要求，从信息系统生存周期的不同阶段，规定了对信息系统进行安全管理评估的原则和模式、组织和活动、方法和设施，提出了信息安全等级保护第一级到第五级的信息系统安全管理评估的要求。
数据安全评估		

GB/T 20984-2007	信息安全技术 信息安全风险评估规范	本标准提出了风险评估的基本概念、要素关系、分析原理、实施流程和评估方法，以及风险评估在信息系统生命周期不同阶段的实施要点和工作形式，
GB/T 31509-2015	信息安全技术 信息安全风险评估实施指南	本标准是对《信息安全技术 信息安全风险评估规范》（GB/T 20984-2007）中各阶段评估工作的细化，适用于从事信息安全风险评估活动的有关组织机构和人员，也可为组织内部进行信息安全风险评估提供指导和参考。
GB/T 33132-2016	信息安全技术 信息安全风险处理实施指南	本标准给出了信息安全风险处理的基本概念、处理原则、处理方式、处理流程以及处理结束后的效果评价等管理过程和方法，并对处理过程中的角色和职责进行了定义。
GB/T 35284-2017	信息安全技术 网站身份和系统安全要求与评估方法	本标准从网络展身份和系统安全两个方面提出要求和评估方法，使得网站标识颁发机构可以评估网站的身份真实性和系统安全，互联网各终端软件厂商可查询网站标识颁发机构验证的标识信息，并以适当的方式展示给网民，以实现网民上网行为的保护，帮助网民有效甄别真假网站，净化网络环境。
GB/T 20009-2005	信息安全技术 数据库管理系统安全评估准则	本标准从信息技术方面规定了按照 GB 17859-1999 的五个安全保护等级对数据库管理系统安全保护等级划分所需要的评估内容。本标

		准适用于数据库管理系统的安全保护等级的评估，对于数据库管理系统安全功能的研制、开发和测试亦可参照使用。
GB/T 35287-2017	信息安全技术 网站可信标识技术指南	本标准定义了一种基于我国自主密码算法、可以承载网站真实信息的可信标识体系框架，并对可信标识对象、可信标识对象管理、可信标识对象获取与验证、数据格式与接口等内容进行了规范。
GB/Z 24364-2009	信息安全技术 信息安全风险管理指南	本标准对信息安全风险管理所涉及的背景建立、风险评估、风险处理、批准监督、监控审查、沟通咨询等不同过程进行了综合姓名书，对信息安全风险管理在信息系统生命周期各阶段的应用做了系统阐述。
预警响应与灾难备份		
GB/T 24363-2009	信息安全技术 信息安全应急响应计划规范	本标准规定了编制信息安全应急响应计划的前期准备，确立了信息安全应急响应计划文档的基本要素、内容要求和格式规范。
GB/Z 20985-2007	信息技术 安全技术 信息安全事件管理指南	本指导性技术文件描述了信息安全事件的管理过程，提供了规划和制定信息安全事件管理策略和方案的指南。
GB/Z 20986-2007	信息安全技术 信息安全事件分类分级指南	本指导性技术文件为信息安全事件的分类分级提供指导，用于

		信息安全事件的防范与处置，为事前准备、事中应对、事后处理提供一个基础指南，可供信息系统和基础信息传输网络的运营和使用单位以及信息安全主管部门参考使用。
GB/T 31500-2015	信息安全技术 存储介质数据恢复服务要求	本标准规定了实施存储介质数据恢复服务所需的服务原则、服务条件、服务过程要求及管理要求。
GB/T 20988-2007	信息安全技术 信息系统灾难恢复规范	规定了信息系统灾难恢复应遵循的基本要求。
GB/T 36957-2018	信息安全技术 灾难恢复服务要求	本标准规定了灾难恢复服务资源配置、灾难恢复服务过程和灾难恢复服务项目管理三个方面的灾难恢复服务要求。
GB/T 37046-2018	信息安全技术 灾难恢复服务能力评估准则	本标准规定了信息系统灾难恢复服务所应遵循的基本原则，明确了信息系统灾难恢复服务组织服务能力的评估机制。
应用系统安全		
GB/T 37002-2018	信息安全技术 电子邮件系统安全技术要求	本标准规定了电子邮件系统信息安全要求，包括电子邮件系统的技术安全要求、管理安全要求和运行安全要求。
GB/T 37094-2018	信息安全技术 办公信息系统安全管理要求	规定了办公信息系统的建设管理、系统运维管理、制度管理和外包管理方面的要求。

GB/T 37095-2018	信息安全技术 办公信息系统安全基本技术要求	本标准规定了办公信息系统的安全基本技术要求。
GB/T 37096-2018	信息安全技术 办公信息系统安全测试规范	规定了办公信息系统的物理环境测试、基础硬件产品测试、基础软件产品测试、网络设施测试以及应用软件系统测试的规范。
移动互联网		
GB/T 35278-2017	信息安全技术 移动终端安全保护技术要求	本标准规定了移动终端的安全保护技术要求，包括移动终端的安全目的、安全功能要求和安全保障要求。本标准适用于移动终端的设计、开发、测试和评估。
GB/T 35281-2017	信息安全技术 移动互联网应用服务器安全技术要求	规定了移动互联网应用服务器的安全技术要求，包括数据安全、业务安全、系统安全、设备安全、协议安全和韵味安全等。
GB/T 34977-2017	信息安全技术 移动智能终端数据存储安全技术要求与测试评价方法	规定了移动智能终端数据存储的安全技术要求、测试评价方法和安全等级划分。
GB/T 34978-2017	信息安全技术 移动智能终端个人信息保护技术要求	规定了移动智能终端的个人信息分类和个人信息的保护原则和技术要求。
物联网		

GB/T 37025-2018	信息安全技术 物联网数据传输安全技术要求	规定了物联网（工控终端除外）数据传输安全分级及基本级和增强级安全技术要求等。
GB/T 37044-2018	信息安全技术 物联网安全参考模型及通用要求	规定了物联网安全参考模型，包括物联网安全对象及各对象的安全责任，并规定了物联网系统的安全通用要求。
工业互联网		
GB/T 36324-2018	信息安全技术 工业控制系统信息安全分级规范	规定了基于风险评估的工业控制系统信息安全等级划分规则和定级方法，提出了等级划分模型和定级要素，包括工业控制系统资产重要程度、存在的潜在风险影响程度和需抵御的信息安全威胁程度,并提出了工业控制系统信息安全四个等级的特征。
云计算		
GB/T 38249-2019	信息安全技术 政府网站云计算服务安全指南	本标准给出了政府网站采用云计算服务过程中，在规划准备、部署迁移、运行管理、服务退出等阶段的安全技术措施和安全管理措施。
GB/T 35279-2017	信息安全技术 云计算安全参考架构	本标准规定了云计算安全参考架构，描述了云计算角色，规范了各角色的安全职责、安全功能组件及其关系。
GB/T 34942-2017	信息安全技术 云计算服务安全能力评估方法	本标准给出了依据GB/T 31168-2014《信息安全技术 云计算服务安全能力要求》开展评估的原则、实施过程以及针对各项具体安全要

		求进行评估的方法。本标准适用于专业技术机构对云服务商安全能力进行评估，也适用于云服务商自评估。
GB/T 31167-2014	信息安全技术 云计算服务安全指南	本标准描述了云计算服务可能面临的主要安全风险，提出了政府部门采用云计算服务的安全管理基本要求，及云计算服务的生命周期各阶段的安全管理和技术要求。本标准为政府部门采用云计算服务，特别是采用社会化的云计算服务提供全生命周期的安全指导，适用于政府部门采购和使用云计算服务，也可供重点行业或企事业单位参考。
GB/T 31168-2014	信息安全技术 云计算服务安全能力要求	本标准描述了以社会化方式为特定客户提供云计算服务时，云服务商应具备的信息安全技术能力。适用于对政府部门使用的云计算服务进行安全管理，也可供重点行业和其他企事业单位使用云计算服务时参考，还适用于指导云服务商建设安全的云计算平台和提供安全的云计算服务。标准分为一般要求和增强要求。根据拟迁移到社会化云计算平台上的政府和行业信息、业务的敏感度及安全需求的不同，云服务商应具备的安全能力也各不相同。
大数据		
GB/T 37873-2019	信息安全技术 大数据安全管理指南	本标准提出了大数据安全管理基本原则，规定了大数据安全需求、数据分类分级、大数据活动的安全要求、评估大数据安全

		风险。
–	信息安全技术 电信领域大数据安全防护实现指南（征求意见稿）	本文件规范了电信领域大数据分类分级，基于电信领域大数据生存周期从管理和技术两方面给出了安全防护的实现指南。

参考文献

[1] 国家工业信息安全发展研究中心,华为.数据安全白皮书[R].贵阳.2021 中国国际大数据产业博览会.2021.

[2] 国发〔2015〕50 号,促进大数据发展行动纲要[S].北京:国务院,2015.

[3] 新华网.绍兴首例“大数据杀熟”案成功维权[EB/OL]. http://www.zj.xinhuanet.com/2021-07/08/c_1127635869.htm.

[4] 北京市海淀区人民法院.腾讯科技(深圳)有限公司与北京智借网络科技有限公司等一审民事判决书[EB/OL].(2018)京 0108 民初 17738 号.https://wenshu.court.gov.cn/website/wenshu/181107ANFZ0BXSK4/index.html?docId=42b24563187a431ba7e5ab0d003b2e66.

[5] 京市海淀区人民法院.腾讯科技(深圳)有限公司与北京智借网络科技有限公司等商标权权属、侵权纠纷二审民事判决书[EB/OL].(2018)京 73 民终 2187 号. https://wenshu.court.gov.cn/website/wenshu/181107ANFZ0BXSK4/index.html?docId=8b6f5cc22c1943b59914ab1b0040cbe7.

[6] 中华新闻网.京东 12G 用户数据泄漏!官方:确实存在已修复[EB/OL].http://news.sohu.com/20161211/n475529281.shtml.

[7] 人民日报.“20 万孩童信息被售案”告破抓获 4 名嫌疑人[EB/OL].http://www.xinhuanet.com/politics/2016-05/06/c_128961444.htm.

[8] 北京市第一中级人民法院.北京机锋科技有限公司执行裁定书[EB/OL].(2021)京 01 执异 48 号. https://wenshu.court.gov.cn/website/wenshu/181107ANFZ0BXSK4/index.html?docId=bbfe709df2ca49cabdd9acf600094fb8.

[9] 观察者网.乌云漏洞报告某易用户数据库疑似泄露[EB/OL].https://www.sohu.com/a/36512959_115479.

[10] 河北省涿州市人民法院.非法获取公民的电话信息 10 万多条一审[EB/OL].(2020)冀 0681 刑初 507 号.https://wenshu.court.gov.cn/website/wenshu/181107ANFZ0BXSK4/index.html?docId=6d01197ce72a4645aaabaced001be2e8.

[11] 河北省涿州市人民法院.非法获取公民的电话信息 10 万多条

二审[EB/OL].（2021）冀06刑终180号.https://wenshu.court.gov.cn/website/wenshu/181107ANFZ0BXSK4/index.html?docId=018e5ecb76924777aacbad19001d1bb0.

[12] 腾讯网.257万条公民银行个人信息被泄露银行行长卖账号.https://news.qq.com/a/20161017/002075.htm

[13] 亿欧智库.圆通40万用户信息泄露背后[EB/OL].https://xueqiu.com/2766276381/165113805.

[14] 新浪综合.广西移动人为造成重大故障80万移动用户手机失联[EB/OL].http://news.idcquan.com/news/125899.shtml.

[15] 浙江省绍兴市越城区人民法院.“瑞智华胜”涉嫌非法窃取用户信息30亿条[EB/OL].(2019）浙0602刑初1143号.https://wenshu.court.gov.cn/website/wenshu/181107ANFZ0BXSK4/index.html?docId=b125d8d9e8914a81abc1ab2c009b6dcd.

[16] 央视网.客户信息被泄露中信银行被银保监会罚款450万元[EB/OL].https://m.gmw.cn/baijia/2021-03/19/1302176444.html

[17] 河南省高级人民法院.中国建设银行股份有限公司汝阳支行、顾三斗储蓄存款合同纠纷再审审查与审判监督民事裁定书[EB/OL].（2019）豫民申6252号.https://wenshu.court.gov.cn/website/wenshu/181107ANFZ0BXSK4/index.html?docId=51a3eaea8a7c427eaf3aaafe0095305e.

[18] 河南省高级人民法院.中国建设银行股份有限公司汝阳支行、顾三斗储蓄存款合同纠纷二审民事判决书.（2019）豫03民终1928号.[EB/OL].https://wenshu.court.gov.cn/website/wenshu/181107ANFZ0BXSK4/index.html?docId=d79ec7c6d77541e0afccac93008df3fe.

[19] 齐鲁晚报.青岛胶州6685人就诊名单被泄露警方回应[EB/OL].http://yuqing.people.com.cn/n1/2020/0416/c209043-31676483.html.

[20] 新浪财经.邯郸丛台区政府网站再度泄露个人隐私，区长回应后网页已撤下[EB/OL].https://baijiahao.baidu.com/s?id=1709513616936410568&wfr=spider&for=pc.

[21] 高伟.数据资产管理-盘活大数据时代的财富[M].北京:机械工业出版社,2016.

[22] 刘潮.一文读懂数据内容识别核心技术[EB/OL].

http://blog.nsfocus.net/data-content-identification-core-technology/.
[23] 亿赛通.浅析数据防泄漏 DLP 的指纹文档比对技术[EB/OL].
http://www.esafenet.com/newsitem/277852284.
[24] 奉国和.四种分类方法性能比较[D].广州华南师范大学,2011.
[25] 傅戈.BIGID 数据沙盒产品及技术解读[EB/OL].
http://blog.nsfocus.net/rsa2018-bigid.
[26] Browser_hot.大数据安全之敏感数据识别和分级打标[EB/OL].
https://blog.csdn.net/u014779378/article/details/103035474/.
[27] 数据库安全.数据安全能力成熟度模型实践指南 01：数据分级分类[EB/OL].https://blog.csdn.net/meichuangkeji/article/details/108333838.
[28] GB/T 37988-2019.《信息安全技术 数据安全能力成熟度模型》[S].全国信息安全标准化技术委员会.2021.
[29] 陈驰,马红霞.赵延帅.基于分类分级的数据资产安全管控平台设计与实现[D].广州.2016.
[30] 杨腾飞,申培松,田雪,冯荣权.对象云存储中分类分级数据的访问控制方法[J].软件学报.2017.
[31] Eleven_Liu.数据库中敏感字段的标记、标示[EB/OL].
https://www.cnblogs.com/Eleven-Liu/p/9912418.html.2018.
[32] 杨腾飞,申培松,田雪,冯荣权.对象关系映射的关键技术研究与实现[J].软件学报.2017.
[33] 丁长松,宁洪.基于 CWM 的企业元数据集成中对象到关系映射模式的研究[J].西南民族大学学报.2006.
[34] 张勇,赵东宁,李德毅.关系数据库数字水印技术[J].计算机工程与应用.2003.
[35] 易开祥,石教英,孙鑫.数字水印技术研究进展[J].中国图象图形学报.2001.
[36] 牛夏牧,赵亮,黄文军,张慧.利用数字水印技术实现数据库的版权保护[J].电子学报.2003.
[37] 唐迪,顾健,张凯悦,顾欣.数据脱敏技术发展趋势[N].保密科学技术杂志,2014.
[38] 刘喻,吕大鹏,冯建华,周立柱.数据发布中的匿名化技术研究综述[D].北京市海淀区:清华大学专利办公室,2007.
[39] GB/T 35273-2020,个人信息安全规范[S].北京:中国国家标准化管理委员,2020.

[40] 杜海涛.口令认证的分类概述[N].科技世界杂志,2011.
[41] GM/T 0100-2020,人工确权型数字签名密码应用技术要求[S].北京:国家密码管理局.2020.
[42] GM/T 0067-2019,基于数字证书的身份鉴别接口规范[S].北京:国家密码管理局.2019.
[43] GB/T 38540-2020,信息安全技术-安全电子签章密码技术规范[S].北京:国家标准化管理委员会,2020.
[44] Steve Riley Craig Lawson.
Magic Quadrant for Cloud Access Security Brokers[R].
[45] 聂元铭,吴晓明,贾磊雷.重要信息系统数据销毁/恢复技术及其安全措施研究[J].信息网络安全.2011.
[46] 崔彦杰.计算机涉密数据销毁的研究与设计[J].科教导刊,2016.
[47] 科来.科来网络全流量安全分析系统.[EB/OL].
http://www.colasoft.com.cn/products/tsa.php.
[48] 安天.探海威胁检测系
统.https://www.antiy.cn/Security_Product/PTD.html.
[49] 何振宇.基于流量分析的HTTP协议安全现状分析[J].科学技术创新 2020.
[50] 百度百科.文件分析法[EB/OL].
https://baike.baidu.com/item/%E6%96%87%E4%BB%B6%E5%88%86%E6%9E%90%E6%B3%95/22625457?fr=aladdin.
[51] 于艳杰.网页文件上传方法分析与研究[J].哈尔滨学院学报.2005.
[52] Gigamon. SSL/TLS 流量解密[EB/OL].
https://www.gigamon.com/cn/products/optimize-traffic/traffic-intelligence/gigasmart/ssl-tls-decryption.html.
[53] 董海韬,田静,杨军,叶晓舟,宋磊.适用于网络内容审计的SSL/TLS保密数据高效明文采集方法.计算机应用.2015.
[54] JR/T0185—2020.商业银行应用程序接口安全管理规范[S].上海：中国人民银行,2020.
[55] GB/T36960—2018.信息安全技术鉴别与授权访问控制中间件框架与接口[S].2021.
[56] 廖年冬,易禹,胡琦.动态实时网络安全风险评估研究[J].维普期刊,2011.
[57] GB/T36466—2018.信息安全技术工业控制系统风险评估实施指南[S].2019.

[58] GB/T 31509—2015.信息安全技术信息安全风险评估实施指南[S].2016.
[59] GB/T 20984—2007.信息安全技术信息安全风险评估规范.
[60] 审计实践.信息安全管理审计.[EB/OL].
https://mp.weixin.qq.com/s?src=11&timestamp=1635491853&ver=3403&signature=B-9XmIErBrXWTudrBCvERbho3BQf9BsHUIgZAeBLPBmcDBGrsyA75yR3d1HFRmYRcBxnjhFbu8pPdrZ31jpC4cbV7Mi4WfVw*GwzWTxqU8x*yDINhFoWM5uLmDsKnbWc&new=1.
[61] 百度文库.浅析网络安全审计原理和技术[EB/OL].
https://wenku.baidu.com/view/e2387a4b5ebfc77da26925c52cc58bd630869332.html.
[62] 百度百科.数据库安全审计系统[EB/OL].
https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E5%BA%93%E5%AE%89%E5%85%A8%E5%AE%A1%E8%AE%A1%E7%B3%BB%E7%BB%9F/8402907?fr=aladdin.
[63] 杜雪娟.浅谈网络安全审计[J].维普期刊.2010.
[64] 美创科技.业务安全审计系统.[EB/OL].http://www.mchz.com.cn/cn/product/BSA/
[65] 黄精籼,庞松健,程治胜,庞萍.基于大数据平台的业务安全审计方法[J].中国新通信.2019.
[66] 山石网科.共享接入监控系统.[EB/OL].
http://docs.hillstonenet.com/cn/Content/11_Monitor/monitor_share_access.htm.
[67] 华为.华为安全免疫网关（SIG）之共享接入监控解决方案[EB/OL].https://wenku.baidu.com/view/0439afd23186bceb18e8bb05.html.
[68] GB/T38645—2020.信息安全技术网络安全事件应急演练指南.2020.
[69] GB/T24363—2009.信息安全技术信息安全应急响应计划规范.2009.
[70] 奇安信安服团队.网络安全应急响应技术实战指南[M].北京:电子工业出版社.2020.
[71] Afra 林红.网络安全应急响应具体措施[EB/OL].
https://zhuanlan.zhihu.com/p/392088325.
[72] 中华人民共和国主席令第八十四号,中华人民共和国数据安全法[S].北京：十三届全国人大常委会公布立法规划,2021.
[73] Bypass.安全攻击溯源思路及案例.[EB/OL].
https://www.cnblogs.com/xiaozi/p/13817637.html.
[74] 刘英,王效武,曾兵.一种数据备份与恢复系统体系设计.维普期期刊.2011.

[75] 尹碧波.关于企业大数据的集群备份技术(ORACLE RAC)的解决方案[J].维普期期刊.2017.

[76] 刘怡多,马明成.浅谈 ORACLE 数据库 RAC 集群备份[J].维普期刊.2013.

[77] 中国信息通信研究院云计算与大数据研究所,北京百度网讯科技有限公司. 金融级数据库容灾技术报告[R]. 2021.

[78] 肖达,刘建毅.灾备关键技术[C].北京:2010.

[79] 陈钊. 基于云灾备的数据安全存储关键技术研究[D]. 北京邮电大学.

[80] 吕帅,刘光明,徐凯等. 海量信息分级存储数据迁移策略研究[J]. 计算机工程与科学, 2009(A01):163-167.

[81] 黄冬梅,杜艳玲,贺琪.混合云存储中海洋大数据迁移算法的研究[J].钛学术.2014.

[82] 胡晓鹏,李晓航,李岗.一种基于 XML 映射规则的数据迁移方法设计和实现[J].维普期刊专业版.2005.

[83] 熊富琴.媒体数字水印技术综述[J].科技信息,2010 年

[84] 王芳,赵洪,马嘉悦,李晓阳,张晓悦.数据科学视角下数据溯源研究与实践进展[N].中国图书馆学报,2019 年第五期.

[85] 王笑笑,郝红军,张树臣,等.基于模糊神经网络的大数据价值评估研究[J].科技与管理,2019,21(02):4-12.

[86] 腾讯云数据派 THU.数据有价——数据资产定价研究初探[EB/OL].https://cloud.tencent.com/developer/article/1513812.

[87] 郑苏瑶,郭树行.面向数据证券化的数据价值评估策略研究[J].科技资讯,2020,018(003):234-235.

[88] 寇怀忠,梁剑辉,朱辰华.数据资源共享与交换的思考与实践——以"数字黄河"工程为例[J].水利信息化,2010(02):24-27.

[89] 宋文凤.科学数据价值鉴定研究[D].吉林大学,2013.

[90] 王卫,王晶,张梦君.生态系统视角下开放政府数据价值实现影响因素分析[J].图书馆理论与实践,2020(1):7.

[91] 宋栋,张雷,苏马婧.基于 AHP-模糊综合评价法的泄露数据价值评估模型[J].信息技术与网络安全,2020,v.39;No.521(09):48-52.

[92] 赵小明,孙晓璇.数据资产估值与收益分配方法研究[J].2021.

[93] MBA 智库百科.信息经济学概述[EB/OL].https://wiki.mbalib.com/wiki/信息经济学.

[94] Speybroeck J V . Infonomics: how to monetize, manage, and measure information as an asset for competitive advantage[J]. Computing Reviews, 2019, 60(6):247-247.

[95] 尹传儒,金涛,张鹏,等.数据资产价值评估与定价:研究综述和展望[J].大数据,2021,7(4):14.

[96] GB/T37550-2019.电子商务数据资产评价指标体系.2020.

[97] 中国信息通信研究院.数据价值化与数据要素市场发展报告[R].2021.

[98] 李洋.Gartner 发布 2019 年十大战略技术趋势数字道德与隐私位列其中[J].互联网天地,2018(10):1.

[99] aqniu 安全牛.Gartner2019 年十大战略技术趋势之一：数字道德与隐私[EB/OL].https://www.aqniu.com/tools-tech/49374.html.

[100] 中国通信企业协会.供应链安全分析[R].2021.

[101] 中国网信网.专家解读｜强化供应链安全保障工作，保护关键信息基础设施安全[EB/OL].http://www.cac.gov.cn/2021-08/31/c_1632032388356198.htm

[102] 王峰.数据安全下的供应链管理建设[EB/OL], https://blog.csdn.net/a59a59/article/details/113795198

[103] YD/T3802-2020.电信网和互联网数据安全通用要求[S].2020.

[104] GB/T37973-2019.信息安全技术大数据安全管理指南[S].2019.

[105] YD/T3801-2020.电信网和互联网数据安全评估技术实施指南[S].2020.

[106] GB/T37988-2019.信息安全技术数据安全能力成熟度模型[S].2019.

作者介绍

炼石网络是一家数据安全技术创新厂商，先后获得安天、国科嘉和、腾讯等投资。炼石提倡“以数据为中心的新安全理念”，核心自研产品是 CASB 数据安全平台，该产品夺得第七届互联网安全大会(ISC 2019)首届“创新独角兽沙盒大赛”总冠军。技术特色是免开发改造应用的数据保护、高性能国产密码和去标识化技术，为政府、金融、运营商、交通、教医旅等用户提供个人信息保护、商业秘密保护、国密合规改造。面向《密码法》《数据安全法》《个人信息保护法》等法律法规，企业重要数据与个人信息亟待提升防护水平与合规改造。炼石基于面向切面数据安全技术，构建高覆盖率的安全增强点组合，融合识别、加密、去标识化、检测/响应、追溯等能力，有效保护结构化与非结构化数据，打造免开发改造的应用级数据安全防护，实现分布式保护、集中式管控，可应用在数据存储、使用、加工、传输、提供等生命周期。炼石方案可在不影响业务的前提下敏捷实施上线，将安全与业务在技术上解耦、但又在能力上融合交织，实现主体到应用内用户、客体到字段级的防护，打造实战化数据安全防护体系。欢迎感兴趣的合作伙伴，随时和我们联系，共同掘金“数据安全市场”。

炼石
CipherGateway

让数据开发利用更安全

www.ciphergway.com

support@ciphergateway.com

400-819-0181