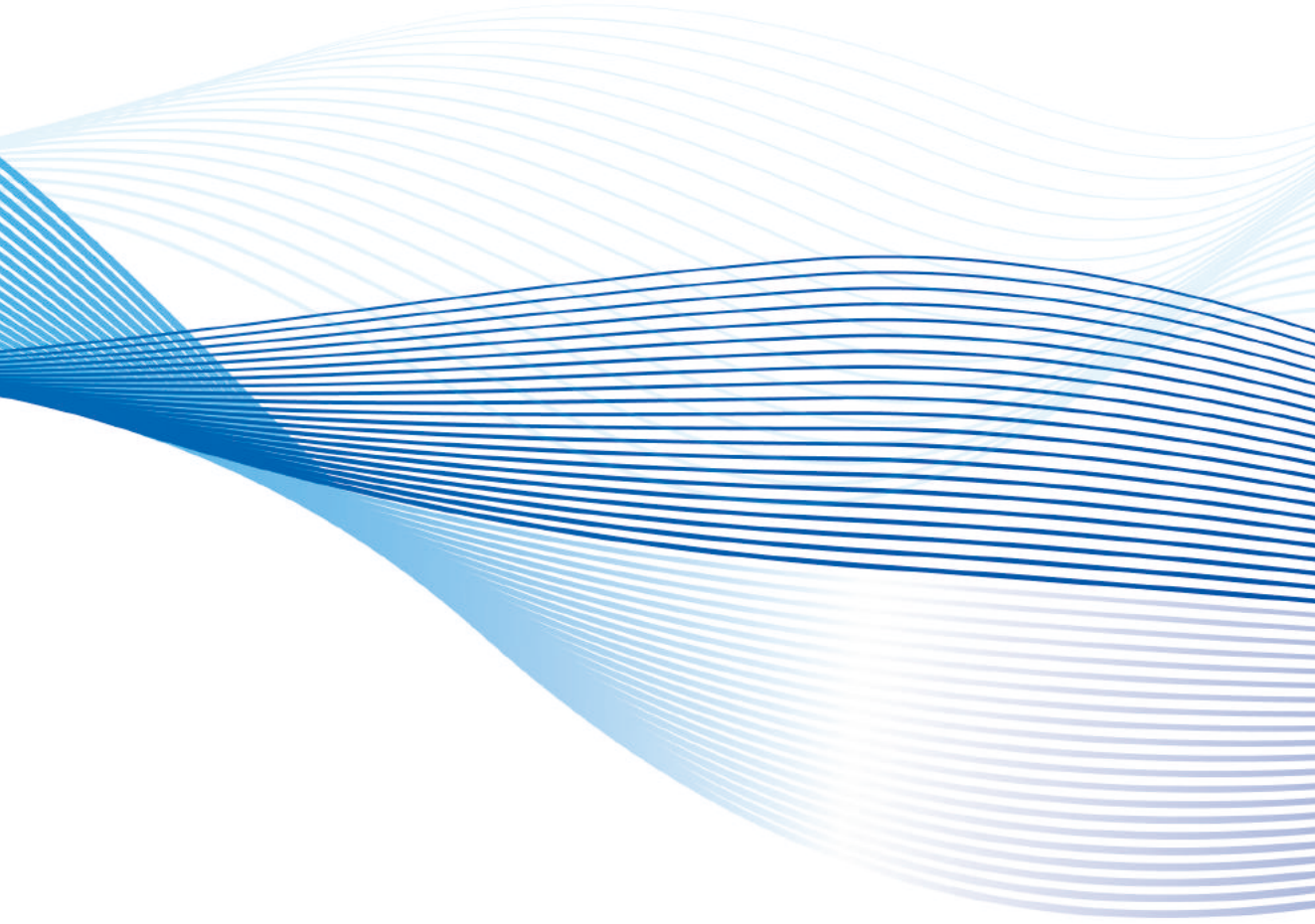
数据传输安全白皮书



工业和信息化部网络安全产业发展中心编写组

2022年7月

编写组

郭　威	王欢欢	陈雨阳	张　旭
李吉音	叶晓丽	宋永豪	朱　岩
李红娟	修佳鹏	钱业斐	王　天
邹　庆	黄加南	王　郁	徐　越

特别感谢支持 （排名不分先后）

中国信息安全研究院
清华大学互联网产业研究院
北京邮电大学
北京交通大学信息安全系
西北工业大学北京研究院
立信会计师事务所（特殊普通合伙）
北京星阑科技有限公司
绿盟科技集团股份有限公司
中信银行股份有限公司科技运营中心
中国光大银行股份有限公司
中信百信银行股份有限公司
中电科智能科技园有限公司
联通智慧安全科技有限公司
金网络（北京）电子商务有限公司
朴道征信有限公司
华为云计算技术有限公司
腾讯云计算 (北京) 有限责任公司
北京沃东天骏信息技术有限公司（京东）
北京微梦创科网络技术有限公司 (微博)
北京快手科技有限公司
北京自如信息科技有限公司
医渡云（北京）技术有限公司
江泰保险经纪股份有限公司
北京神州云合数据科技发展有限公司
万帮数字能源股份有限公司
北京明朝万达科技股份有限公司
深圳鼎铉数字科技控股有限公司
广东一知安全科技有限公司
成都云山雾隐科技有限公司等
北京北斗弘鹏科技有限公司
渔翁信息技术股份有限公司

目录

CONTENTS

CONTENTS

一、形势和挑战

数据已成为关键生产要素，是数字经济创新发展的“石油”。与此同时，数据安全成为全球关注焦点，面临更多风险挑战。

1.1 数据安全成为全球关注焦点

随着数字化浪潮席卷全球，各国政府逐渐意识到，数据已成为与国家安全和国际竞争力紧密关联的重要资源要素，对数据安全的认知已从传统的个人隐私保护上升到维护国家安全的高度。各行业各领域企业内生发展需求和外部合规要求激增，正在积极利用新技术不断提升数据安全保障能力。

从顶层设计来看，美国国防部发布《国防部数据战略》，指出战略的核心目标之一就是通过构建访问控制和最严格的安全标准来保护国防部数据安全，以实现数据推动作用下的联合全域作战，构筑国家安全保护屏障；英国发布《国家数据战略》，通过搭建国家层面的数据安全治理方案，为建设促进增长和可信赖的数据机制提供指导方向，保障国家安全；欧盟委员会相继发布《欧洲数据战略》及其配套法案《数据治理法案》提案，力求在欧盟层面建立统一的数据治理框架，保障数据安全。

从监管立法来看，美国发布《联邦数据战略与2020年行动计划》，确立了保护数据完整性、确保流通数据真实性、数据存储安全性等基本原则；2018年，欧洲联盟生效通过《通用数据保护条例》（“GDPR”），堪称史上数据安全保护力度最大的法律，后相继发布《欧洲数据保护监管局战略计划（2020-2024）》等，旨在从前瞻性、行动性和协调性三方面继续加强数据安全保护，保证个人隐私的基本权利；阿联酋迪拜和新西兰分别出台《数据保护法》和《2020年隐私法》，加强对数据安全及个人隐私保护的规制建设；日本和新加坡分别完成了对本国《个人信息（数据）保护法》的修订，明确了个人数据权利及外部使用限制；加拿大提出《数字宪章实施法案2020》，提出了保护私营部门个人信息的现代化框架。

从落地实施来看，美国商务部成立提供联邦数据服务的咨询委员会，加强联邦数据隐私保护；巴西总统签署法令批准建立国家个人数据保护局，负责制定相关规则、推进企业开展数据安全风险评估、调查违法违规行为、促进数据保护国际合作等；韩国成立个人信息保护委员会，负责个人信息保护与监管执法工

作；欧盟发布《为保持欧盟个人数据保护级别而采用的数据跨境转移工具补充措施》，为数据跨境流动中数据保护问题提供了进一步指导；西班牙数据保护局发布《默认数据保护指南》，阐释了默认数据保护原则的策略、实施措施、记录和审计要求等，为企业实践数据保护原则提供具体指导。

从惩治力度来看，随着大型互联网平台企业的日益壮大，其数据垄断问题愈加严重，由此带来的权利滥用问题或将威胁到国家安全。美国、欧洲等国家和地区均对大型互联网企业数据安全违法违规行为增大了单笔处罚金额，防止其滥用数据优势侵害消费者隐私或进行非法数据贩卖。例如，因Facebook违反用户隐私保护策略，美国对其处以50亿美元巨额罚款；爱尔兰也就数据非法跨境传输问题，对Facebook处以了高达28亿美元的罚款；法国、加拿大等国家也纷纷对Twitter、谷歌等企业开出高额罚单。

为保障基础设施建设，防止数据滥用，我国对大型互联网企业的数据安全违法违规行为做出了严峻的惩罚。例如，滴滴全球股份有限公司因违反《网络安全法》、《数据安全法》、《个人信息保护法》，危害国家网络安全、数据安全、侵害公民个人信息等相关违法行为，国家网信办对滴滴全球股份有限公司处以人民币80.26亿元罚款，对滴滴全球股份有限公司董事长兼CEO程维、总裁柳青各处以人民币100万元罚款。

从技术创新来看，全球数据量出现爆炸式增长，各领域各行业的企业结合自身发展路径，按照当地法律法规等各类合规要求，从数据处理的主体客体、数据传输通道、数据运营管理等方面入手，积极运用差分隐私、区块链等创新技术手段，搭建具有鲜明数据安全保护特性的技术架构，持续提升数据安全意识，不断强化数据安全保护。例如，Facebook通过开源差分隐私库加强对人工智能训练样本隐私性的保护；苹果公司通过模糊定位技术限制第三方App获取用户精确地理位置信息；亚马逊推出阻止用户敏感信息泄露的服务Macie，保护企业云端敏感数据；新西兰企业通过区块链技术实现数据加密传输和追踪溯源，保护数据安全。

1.2 数据安全面临更多风险挑战

·管理战略重视不够，统筹协调力度有待加强。数据安全实践由单个部门（如安全部门、信息化部门等）主导，是比较普遍的共性现象。由于在战略层面缺少足够的顶层支持和驱动，难以建立起全面完善的安全治理组织架构和制度规范体系，导致工作职责划分不明确、安全机制难落实等突出问题，数据安全仅能在部分关键业务或部门有限范围内实施保障，难以面向整个组织有效开展。

·管理过程较离散化，缺少全局引领与监督评价。在实践中，容易以解决特定数据安全问题为导向的离散化、补丁式管理方式推进，缺少对数据安全管理体系的全局思考与规划。管理过程中重制定轻落实的现象比较突出，制度追求大而全，内容过于宽泛，缺乏可落地性和可实施性。缺少直接以数据为对象的针对性安全评估和红蓝演练，安全风险和薄弱环节的主动发现和应对处置能力偏弱。

·安全先行意识不强，与业务融合程度亟待提升。数据安全的有效实施离不开科学规划与全员深度参与。组织在对业务、产品等进行规划设计的阶段对数据安全考量不够充分，与业务、产品全流程融合度不足，针对数据安全核心元素“人”的管理不够，培训方式较为单一，培训内容针对性不强，缺少对培训效果的评价考核，难以形成有效的覆盖组织全员的数据安全意识提升。

·泄密风险难以避免，实时监测管控和溯源追责难。在日常工作中，不可避免的要通过即时通讯工具、网络、邮件等方式发送敏感数据，如：合同、财务报表、知识产权、技术研发、设计、归档管理资料等，在互联网上数据的外发风险时刻存在，并可能造成重大数据泄露事故。一方面，对内部敏感数据的分布、流向、外发等情况难以实时跟踪态势；另一方面，在发生泄密事件后，有效溯源和清晰追责更是难度较大。

- 敏感数据分布在组织的各个角落；
- 敏感数据泄露可能发生在组织中的任何人身上；
- 敏感数据的泄露可能发生在任何时间；
- 敏感数据的传输风险可能发生在任何一种网络应用中。

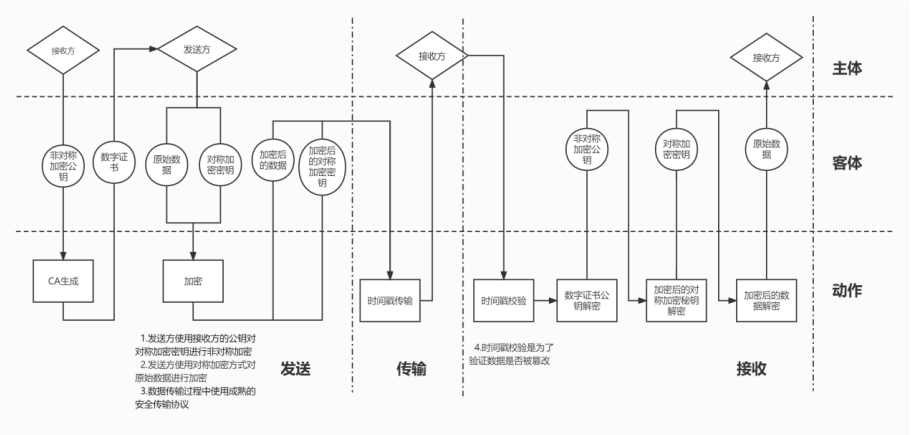
二、概念界定和范围

数据传输安全，是指通过采取必要措施，确保数据在传输阶段，处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

2.1 界定和范围

在2021年9月1日正式施行的《中华人民共和国数据安全法》第一章第三条中，明确将数据定义为任何以电子或者其他方式对信息的记录；将数据处理定义为数据的收集、存储、使用、加工、传输、提供、公开等；将数据安全定义为通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

为了便于研究与交流，在此采纳上述文件中的相关定义。同时，结合数据安全相关法律法规和产业调研，本白皮书认为数据传输安全，是指通过采取必要措施，确保数据在传输阶段，处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。



从管理方面入手

通过制定数据安全规则、开展员工安全培训等方式提升数据传输安全意识；
明确规范操作流程，减少由人为操作失误而造成的数据传输安全问题。

从技术方面入手

利用加密技术对数据进行加密，保护传输的数据安全；
利用身份鉴别技术确认传输节点身份，保证传输的节点安全；
使用成熟的安全传输协议，保证传输的通道安全。

2.2 作用意义

随着新一代信息技术的迭代发展和数字经济的快速推进，各类数据海量汇聚，数据安全问题日益凸显，成为关系国家安全和经济社会发展，关系广大人民群众切身利益的重大问题。数据传输安全作为数据全生命周期安全的关键环节，对于保障数据整体安全有着重要的意义。

从国家层面看，保障数据传输安全是保护数据安全，维护国家安全，保障数字经济健康发展，推动构筑国家竞争新优势的重要部分。对国家安全而言，保障数据传输安全与国家公共服务、社会治理、经济运行、国防安全等方面密切相关，个人信息、企业经营管理数据和国家重要数据的流动，尤其是跨境流动，存在多种安全风险挑战；对数字经济而言，随着新一轮科技革命和产业变革的加快推进，数据作为新型生产要素，有效促进数字基础设施发展与产业迭代升级，数字经济已成为我国经济高质量发展的新引擎，保障数据传输安全，已成为我国数字经济蓬勃发展的关键所在；对国家竞争优势而言，发展数字技术、数字经济，加强数据治理，综合运用政策、监管、法律等多种手段确保数据安全和有序流动，是全球科技革命和产业变革的先机，是新一轮国际竞争重点领域，是构筑国家竞争新优势的重要因素。保障数据传输安全已经为维护国家主权、安全和发展利益不可所缺的重要部分。

从企业层面看，保障数据传输安全对于保护企业数据安全，维护企业经济利益、竞争力以及持续经营能力有着重要意义。在数字化转型大趋势下，数据已成为企业日常办公、生产经营、技术创新、战略发展等活动的基础，数据安全已成为数字企业健康稳定发展的基本保证。目前，数据在传输过程中面临着传输主体多样、处理活动复杂、攻击手段升级、内部泄露频发等安全风险挑战。保障数据在传输过程中的安全性、完整性和可用性，对于维护企业业务连续性，保护企业竞争力、经济利益，确保企业安全转型和持续健康发展有着重要意义。

从个人层面看，保障数据传输安全对于保护个人信息安全，维护个人合法权益和人身安全有着重要作用。在数字社会中伴随日常活动，会产生大量个人数据，反之这些数据也能反映个人活动的方方面面。保障个人数据传输安全，确保个人数据在传输过程中不被篡改、破坏、泄露、窃取和非法利用，关系到个人的隐私权、决定权、知情权、人格权等多种权利，甚至关系到个人财产和人身安全。通过采取必要措施保护个人数据传输安全，能更加全面地保护个人信息安全，维护数字社会中个人的人格尊严和自由，保障个人合法权利、利益与人身安全不受侵害。

三、政策梳理

随着《数据安全法》正式发布，数据安全工作首次升至国家安全最高监管层级，数据传输安全相关法律法规体系日益完善。

3.1 国家层面

2014年2月27日，中共中央成立中央信息安全与信息化领导小组，由习近平任组长，李克强、刘云山任副组长。习近平主席在小组成立时的讲话中指出：“没有网络安全，就没有国家安全”。在国家顶层战略引导下，我国在国家安全、网络安全、数据安全与个人信息保护、关键信息基础设施、数据安全与个人信息保护、车联网多个领域密集出台了多项信息安全法律法规和政策文件，有效促进了信息安全领域的技术创新和应用落地，为筑牢国家信息安全屏障、推进网络强国建设提供了有力支撑。

数字经济时代背景下，更多的数据开始从个人与组织中被提取出来，经过分析和处理后，进入公共通信和信息服务、电子政务、公共服务、金融、交通、能源、水利等重要行业和领域，成为重要的数据资产。这些行业和领域属于关键信息基础设施，是经济社会运行的神经中枢，是网络安全的重中之重。保障关键信息基础设施的安全，对于维护国家网络安全、网络空间主权和国家安全、保障经济社会健康发展、维护公共利益和公民合法权益都具有十分重大的意义。

目前从整体来看，我国数据安全相关法律体系日趋完善，但数据传输安全方向的法律体系尚不完整，法域不宽广，结构内容不丰富。在数据传输安全的重要性日益突显的今天，我国应该在思想观念、结构布局、体制机制等方面做好顶层设计，发挥法治对数据传输安全的规范和保障作用，尽快从国家层面制定相关法律细则，构建和完善数据传输安全法律体系。

2015年7月1日，我国公布并施行了《国家安全法》，第二十五条提出，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，《网络安全法》施行，第七十六条明确，网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

2020年1月1日，《密码法》施行，为规范密码应用和管理，促进密码事业发展，保障网络与信息安全，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益，提供有效法律支撑。通过立法提升密码管理科学化、规范化、法治化水平，促进我国密码事业的稳步健康发展。

2021年1月1日，《民法典》施行，第一百一十一条强调，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。

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》通过，第十八章提出，统筹数据开发利用、隐私保护和公共安全，加快建立数据资源产权、交易流通、跨境传输和安全保护等基础制度和标准规范。

2021年9月1日，《数据安全法》施行，第三条明确，数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

2021年9月1日，《关键信息基础设施安全保护条例》施行，第六条要求，运营者依照本条例和有关法律、行政法规的规定以及国家标准的强制性要求，在网络安全等级保护的基础上，采取技术保护措施和其他必要措施，应对网络安全事件，防范网络攻击和违法犯罪活动，保障关键信息基础设施安全稳定运行，维护数据的完整性、保密性和可用性。

2021年11月1日，《个人信息保护法》施行，第四条明确，个人信息是以电子或

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。个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

《民法典》《数据安全法》《个人信息保护法》相继施行，标志着我国以数据安全保障数据开发和利用产业的健康有序发展全面进入法治化轨道，重要数据及个人信息保护成为时代需求。从相关法律的发布进程来看，我国数据安全领域的政策体系不断完善，基础法规架构已初步构建完成，数据安全产业将迎来发展的黄金期。

3.2 部委层面

从部委层面来看，网信办、工信部、财政部、商务部、国家安全部等各部门发布相应规定，对数据安全问题都愈加重视。但对于数据传输安全并没有单独发布相关政策法律法规，只在数据安全相关文件中涉及了部分数据传输安全问题。

从各部委发布的政策数量分布来看，工业和信息化部发布了数据安全相关政策共32份，其中有8份涉及数据安全传输问题。

2016年底发布的《工业和信息化部关于印发大数据产业发展规划(2016－2020年)的通知》中强调，发挥企业创新主体作用，整合产学研用资源优势联合攻关，研发大数据采集、传输、存储、管理、处理、分析、应用、可视化和安全等关键技术。2019年12月发布的《网络预约出租汽车经营服务管理暂行办法下》则在第二十七条中要求，网约车平台公司不得利用其服务平台发布法律法规禁止传播的信息，不得为企业、个人及其他团体、组织发布有害信息提供便利，并采取有效措施过滤阻断有害信息传播；发现他人利用其网络服务平台传播有害信息的，应当立即停止传输，保存有关记录，并向国家有关机关报告。

2020年5月发布的《工业和信息化部关于工业大数据发展的指导意见》，在加强工业数据安全产品研发的部分中，明确要开展加密传输、访问控制、数据脱敏等

安全技术攻关，提升防篡改、防窃取、防泄露能力。加快培育安全骨干企业，增强数据安全服务，培育良好安全产业生态。

2020年底发布的《电信和互联网行业数据安全标准体系建设指南》，从数据采集、传输、存储、处理、交换、销毁等全生命周期环节出发，对数据安全的关键技术进行规范；并明确数据传输标准用于规范数据传输过程中可以标准化的功能架构、安全协议及其他安全相关技术要求，主要包括数据传输完整性保护、数据加密传输等标准。

2021年9月发布的《关于加强车联网网络安全和数据安全工作的通知》强化车载通信设备、路侧通信设备、服务平台等安全通信能力，采取身份认证、加密传输等必要的技术措施；加强在线升级服务安全校验能力，采取身份认证、加密传输等技术措施，保障传输环境和执行环境的网络安全；提升数据安全技术保障能力，要采取合法、正当方式收集数据，针对数据全生命周期采取有效技术保护措施，防范数据泄露、毁损、丢失、篡改、误用、滥用等风险；各相关企业要强化数据安全监测预警和应急处置能力建设。

2021年4月发布的《智能网联汽车生产企业及产品准入管理指南（试行）（征求意见稿）》则要求，采取有效技术措施，强化数据采集、传输、存储、使用等安全保护，及时处置数据泄露、滥用等安全事件。

2022年2月10日第二次公开发布《工业和信息化领域数据安全管理办法（试行）》（征求意见稿）要求，工业和信息化领域数据处理者应当根据传输的数据类型、级别和应用场景，制定安全策略并采取保护措施；传输重要数据和核心数据的，应当采取校验技术、密码技术、安全传输通道或者安全传输协议等措施。

2021年12月22日发布的《工业和信息化领域数据安全风险信息报送与共享工作指引（试行）（征求意见稿）》，明确了违规传输，包括但不限于数据未按照有关规定擅自进行传输等相关风险。

国家互联网信息办公室发布了数据安全相关政策共26份，其中有6份涉及数据安全传输问题。

2019年2月发布的《金融信息服务管理规定》中第十一条要求，金融信息服务提供者发现含有本规定第八条所列信息内容的，应当立即终止传输、禁止使用和停止传播该信息内容，及时采取处置措施，消除相关信息内容，保存完整记录并向国家或地方互联网信息办公室报告。

2019年11月发布的《App违法违规收集使用个人信息行为认定方法》，明确了既未经用户同意，也未做匿名化处理，数据传输至App后台服务器后，向第三方提供其收集的个人信息，可被认定为“未经同意向他人提供个人信息”。

2021年1月发布的《互联网信息服务管理办法（修订草案征求意见稿）》中则对传输的信息类别、上报机关等方面做出要求。

2021年10月发布的《互联网用户账号名称信息管理规定（征求意见稿）》，明确了未经互联网用户账号使用者授权同意，不得收集、存储、使用、加工、传输、提供或者公开个人信息及账号名称信息。

2021年11月发布的《网络数据安全管理条例（征求意见稿）》，在加强数据处理系统、数据传输网络、数据存储环境等安全防护方面做出要求；同时，明确任何个人和组织不得提供用于穿透、绕过数据跨境安全网关的程序、工具、线路等，不得为穿透、绕过数据跨境安全网关提供互联网接入、服务器托管、技术支持、传播推广、支付结算、应用下载等服务。

此外，2019年8月国家互联网信息办公室还联合市场监管局等八部门发布了《关于引导规范教育移动互联网应用有序健康发展的意见》，并在规范数据管理方面，明确教育移动应用提供者应当建立覆盖个人信息收集、储存、传输、使用等环节的数据保障机制。

发文单位	发文时间	政策名称	内容概述
工业和信息化部	2016/12/18	《工业和信息化部关于印发大数据产业发展规划（2016－2020年）的通知》	安全规范。安全是发展的前提，发展是安全的保障，坚持发展与安全并重，增强信息安全技术保障能力，建立健全安全防护体系，保障信息安全和个人隐私。加强行业自律，完善行业监管，促进数据资源有序流动与规范利用。
国家互联网信息办公室	2019/2/1	《金融信息服务管理规定》	金融信息服务提供者应当履行主体责任，配备与服务规模相适应的管理人员，建立信息内容审核、信息数据保存、信息安全保障、个人信息保护、知识产权保护等服务规范。
教育部、工业和信息化部、中央网络安全和信息化委员会办公室公 安部、民政部、国家市场监督管理总局、国家新闻出版署、全国扫黄打非工作小组	2019/8/10	《关于引导规范教育移动互联网应用有序健康发展的意见》	保障网络安全。教育移动应用提供者应当落实网络安全主体责任，采取有效措施，防范应对网络攻击，保障系统的平稳、安全运行。教育移动应用和后台系统应当统一落实网络安全等级保护要求。应用商店等移动应用分发平台提供者应当加强教育移动应用上架审核管理，建立开发者真实身份信息登记制度，对教育移动应用开展安全审核，及时处理违法违规教育移动应用。鼓励教育移动应用提供者参加网络安全认证、检测，全面提高网络安全保障水平。

发文单位	发文时间	政策名称	内容概述
工业和信息化部	2019/9/4	《工业大数据发展指导意见（征求意见稿）》	构建工业大数据安全保障体系。明确安全主体责任和防护要求，构建形成覆盖工业大数据全产业链的安全管理体系。加强工业大数据态势感知、测试评估、预警处置等保障能力建设。指导企业加大安全投入，建立企业自身大数据安全风险防控体系，确保涉及企业商业秘密、公共利益、国家安全等重要敏感数据的安全。
国家互联网信息办公室秘书局、工业和信息化部办公厅、公安部办公厅、国家市场监督管理总局办公厅	2019/11/28	《App 违法违规收集使用个人信息行为认定方法》	根据《关于开展 App 违法违规收集使用个人信息专项治理的公告》，为监督管理部门认定 App 违法违规收集使用个人信息行为提供参考，为 App 运营者自查自纠和网民社会监督提供指引，落实《网络安全法》等法律法规，制定了该方法。
交通运输部、工业和信息化部、公安部、商务部、国家市场监督管理总局、国家互联网信息办公室	2019/12/28	《网络预约出租汽车经营服务管理暂行办法》	网约车平台公司应当加强安全管理，落实运营、网络等安全防范措施，严格数据安全保护和管理，提高安全防范和抗风险能力，支持配合有关部门开展相关工作。
工业和信息化部	2020/4/28	《关于工业大数据发展的指导意见》	加强工业数据安全产品研发。开展加密传输、访问控制、数据脱敏等安全技术攻关，提升防篡改、防窃取、防泄露能力。加快培育安全骨干企业，增强数据安全服务，培育良好安全产业生态。

发文单位	发文时间	政策名称	内容概述
工业和信息化部	2020/12/17	《电信和互联网行业数据安全标准体系建设指南》	为落实《中华人民共和国网络安全法》《全国人民代表大会常务委员会关于加强网络信息保护的决定》《电信和互联网用户个人信息保护规定》等法律法规要求，指导电信和互联网行业数据安全标准化工作，工业和信息化部组织制定了该指南。
国家互联网信息办公室	2021/1/8	《互联网信息服务管理办法（修订草案征求意见稿）》	互联网信息服务提供者、互联网网络接入服务提供者及其工作人员对所收集、使用的身份信息、日志信息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，防止所收集、使用的身份信息、日志信息泄露、毁损、丢失。在发生或者可能发生信息泄露、毁损、丢失的情况时，应当立即采取补救措施，并按照规定及时告知用户并向有关主管部门报告。
工业和信息化部	2021/4/7	《智能网联汽车生产企业及产品准入管理指南(试行)(征求意见稿)》	企业应建立完善数据安全管理制度,实施数据分类分级管理，制定重要数据目录，强化数据访问权限管理和安全审计；采取有效技术措施，强化数据采集、传输、存储、使用等安全保护，及时处置数据泄露、滥用等安全事件。

发文单位	发文时间	政策名称	内容概述
工业和信息化部	2021/9/15	《关于加强车联网网络安全和数据安全工作的通知》	提升数据安全技术保障能力。智能网联汽车生产企业、车联网服务平台运营企业要采取合法、正当方式收集数据，针对数据全生命周期采取有效技术保护措施，防范数据泄露、毁损、丢失、篡改、误用、滥用等风险。各相关企业要强化数据安全监测预警和应急处置能力建设，提升异常流动分析、违规跨境传输监测、安全事件追踪溯源等水平;及时处置数据安全事件，向所在省（区、市）通信管理局、工业和信息化主管部门报告较大及以上数据安全事件，并配合开展相关监督检查，提供必要技术支持。
工业和信息化部	2022/2/10	《工业和信息化领域数据安全管理办法（试行）》	为了规范工业和信息化领域数据处理活动,加强数据安全管理，保障数据安全，促进数据开发利用，保护个人、组织的合法权益,维护国家安全和发展利益，根据《中华人民共和国民法典》《中华人民共和国数据安全法》《中华人民共和国网络安全法》等法律法规，制定该办法。

发文单位	发文时间	政策名称	内容概述
国家互联网信息办公室	2021/10/26	《互联网用户账号名称信息管理规定（征求意见稿）》	互联网用户账号服务平台应当采取必要措施，确保其收集、存储的个人信息及账号名称信息安全，防止未经授权的访问及信息泄露、篡改、丢失；未经互联网用户账号使用者授权同意，不得收集、存储、使用、加工、传输、提供或者公开个人信息及账号名称信息。不得非法买卖互联网用户账号名称信息。
国家互联网信息办公室	2021/10/29	《数据出境安全评估办法（征求意见稿）》	为了规范数据出境活动，保护个人信息权益，维护国家安全和社会公共利益，促进数据跨境安全、自由流动，根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律法规，制定了该办法。
国家互联网信息办公室	2021/11/14	《网络数据安全管理条例（征求意见稿）》	为了规范网络数据处理活动，保障数据安全，保护个人、组织在网络空间的合法权益，维护国家安全、公共利益，根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律，制定了该条例。
工业和信息化部	2021/12/22	《工业和信息化领域数据安全风险信息报送与共享工作指引（试行）（征求意见稿）》	为加强工业和信息化领域数据安全风险信息获取、分析、研判和预警工作，及时掌握工业和信息化领域数据安全整体态势，提高数据安全风险处置能力，根据《中华人民共和国数据安全法》等法律法规制定了该指引。

四、合规要点

数据传输加密、数据传输端点安全、数据传输访问控制等合规要点逐步明确，相关主体积极响应国家政策，主动应对，探索实践。

4.1 数据传输加密

数据传输过程的数据加密，是确保数据传输安全最有效的技术之一。数据传输加密包括网络通道加密和信源加密，其中网络通道加密包括基于SSL和IPSEC协议的VPN技术，依托协议中的加密和认证技术，实现对网络数据包的机密性和完整性保护，满足移动办公接入、安全组网等需求。信源加密会在数据流动之前先应用加密技术进行加密，在接收端对加密的数据进行解密。每一次两点之间的数据传输过程，都会有加密及解密的过程，一个数据到达目的地之前，可能会经过很多的传输链路，也会经历很多加解密的过程。在线加密技术可以有效确保在网络传输过程的数据流是处于非明文状态，纵使被黑客拦截，也可以有效保障数据安全性，防止非授权用户的搭线窃听和入网，以及数据传输过程中被窃取和篡改。这是比较成熟的技术方案，但在实践应用过程，需要结合以下要点综合全面考虑环境部署。

·数据机密性

数据传输过程的数据机密性，即传输的数据不能明文，这是数据传输安全最基本的要求。常见的数据加解密算法有以下几种：对称算法(国产算法SM1、SM4，国际算法DES、3DES、AES)，非对称算法（国产算法SM2，国际算法RSA）以及哈希算法(国产算法SM3，国际算法SHA512)。对称算法加解密优点是加密解密的速度快，适合于大量数据的加密；非对称算法的加解密效率低，一般也没有必须用于大量数据的加密，通常可以用于数据加密秘钥交换的加密。一般数据传输过程，采用TLS、SSH等加密协议，可以认为数据传输过程中数据保密性合规。

这些加密算法应用非常成熟，组织在应用加密技术时，不能以技术至上，需要从整个组织的角度，综合考量技术与经济效率的平衡，围绕“价值-风险”双元统一的风险管理思想，在保障数据传输安全基本要求的前提下，做出适合组织实际应用的决策。组织并不会使用单一的加密技术，往往会各类技术混合使用、互补优缺点使数据的传输更加安全。

·数据完整性

数据传输过程的数据完整性，可以通过校验技术或密码技术来检测包括鉴别数据、业务数据、审计数据、配置数据、重要个人信息、网络数据等数据，确保数据正常传输、不掉包、传输过程未被篡改以及非授权访问。数据传输过程一般会通过协议来实现数据报文的完整性校验。如数据传输应用TLS、SSH协议，会通过MAC来校验，可以认为数据传输过程中数据完整性合规。

·数据可用性

数据传输过程的数据可用性，主要为了保障对数据的持续访问以及当数据遭受意外攻击或破坏时，可以迅速恢复并能投入使用。具体包括为了避免网络设备以及通信线路出现故障时引起数据通信中断，针对关键链路采用冗余技术设计等手段增强数据访问的可靠性；为保障应用场景下的业务连续性，实现冗余系统的平稳及时切换，快速恢复运行，尽可能减少数据传输的中断时间，例如通过磁盘阵列、数据备份、异地容灾等手段，以规避硬件故障、软件故障、环境风险、人为故障、自然灾害等风险，确保合法用户可以对信息和资源的顺利的使用。

近两年来，在政策驱动和需求牵引的共同作用下，隐私计算技术创新与落地应用快速推进。隐私计算是涉及密码学、统计学、人工智能、计算机硬件等多学科交叉融合的技术体系，具体是指由两个或多个参与方在不泄露原始数据的前提下，通过硬件可信执行环境、联邦学习、多方安全计算等技术手段，保障数据在使用、加工、传输、提供、公开等数据处理活动中的“可用不可见”，保护数据不透明、不泄露、无法被恶意攻击及被其他非授权方获取，同时满足数据开放共享和数据安全保护的双重要求，最终产生超出自身原始数据的更高价值。

4.2 数据传输端点安全

一般来说，应用加密技术能够有效确保数据存储安全。但是在实践中，对所有

数据存储使用加密解密技术，会影响业务数据访问时效性，尤其是高频交互数据。因此，通过对数据传输端点搭建有效的安全防护体系，选取关键增强点进行加密，也是组织在实践中应用比较多的数据安全方案，主动防御数据不被篡改或泄露。

·应用服务器到数据库

数据可分为结构化数据和非结构化数据，结构化数据存储于数据库，例如组织的人事资料、财务数据、销售采购数据等，一般会存储于数据库。数据库是一个应用系统、平台系统最核心的部分，随着数据的资产化，组织最重要的资产在于数据库。应用服务器数据流转到数据库，可以进行前置代理加密以及后置代理加密技术在数据出口第一时间进行数据加密。数据库加密网关，是数据库前置代理加密技术的一种，一般是独立的组件产品，部署在数据库服务器及应用服务器之间，解析数据库协议，在数据保存到数据库之前对敏感数据进行加密，并将密文存储于数据库中，从而起到保护数据安全的效果。

·应用服务器到互联网

常见的应用服务器系统有Web服务器、FTP服务器以及邮件服务器，这些服务器均需要发布到互联网让用户进行访问。Web服务器通过HTTP协议规范了浏览器和Web服务器通信数据的格式，FTP服务器通过FTP协议实现服务器与客户端之间的文件传输及共享，邮件服务器则通过SMTP及POP协议与客户端进行收发邮件。但HTTP协议、FTP协议是以明文方式进行数据传输，没有提供任何方式的数据加密。如果攻击者截取终端与服务器之间的报文，将存在巨大的的安全隐患。因此，目前多数服务器会在应用层协议与TCP/IP协议间，增加SSL协议，保障数据传输安全合规。

·应用服务器到终端

除了上述通过安全通信协议来确保应用服务器到互联网的数据传输安全之

外，组织还会通过安全代理网关来进一步加强访问终端与应用服务器之间的传输安全。常见的安全代理网关，如CASB代理网关，是利用云访问安全机制的委托式安全代理技术，不需要改造目标应用，通过适配目标应用，对客户端请求进行解析，并分析出包含的敏感数据，结合用户身份，通过安全策略对访问请求进行脱敏等控制来进行数据传输的安全管控。

4.3 数据传输通道安全

· 代理服务器到终端

基于SSL协议的传输加密技术主要应用于传输层的安全，采用密码算法和数字证书认证技术，确保登录用户的身份安全可信，以及数据传输的机密性、完整性，满足固定台式终端、移动办公用户、移动智能终端等不同场景、不同平台的可信接入需求。

· 代理服务器到互联网

https在http的基础上加入了SSL协议，SSL依靠证书来验证服务器的身份，并为浏览器和服务器之间的通信加密。可信安全SSL站点证书用于标识网站真实身份，它能够实现网站身份验证，确保用户访问网站的真实性，确保用户所浏览的信息是真实的网站信息，能有效防范假冒网站和钓鱼网站。

代理服务器到代理服务器

基于IPSEC协议的传输加密技术主要应用于网络层IP包传输的安全，包括传输模式和隧道模式，也就是网络层的安全传输。采用密码算法对用户报文进行加密，采用ESP协议对用户报文进行重新封装，确保用户信息传输安全，满足不同分支机构之间以及分支机构与总部之间的加密组网需求。

4.4 数据传输访问控制

除了数据传输过程中对数据本身的安全考量，对数据进行访问控制管理，也能够有效控制数据传输安全。数据传输访问控制可以防止非授权人员访问、修改、篡改以及破坏系统资源，防止数据遭到恶意破坏。访问控制主要有以下实现方式。

·身份认证

身份认证访问控制是指通过身份认证技术限制用户对数据或资源的访问。常见的身份认证方式，包括口令认证技术、双因素身份认证技术、数字证书的身份认证技术、基于生物特征的身份认证技术、Kerberos 身份认证机制、协同签名技术、标识认证技术等。常见的身份认证访问控制应用场景，包括：已经离职以及在职时采用生理特征进行访问控制的员工，应于离职后及时删除基于生物特征录入的信息；外部人员访问时应进行身份认证来进行访问控制；数据处理中心的物理安全也应进行身份认证来进行访问控制，如机房门口应配置电子门禁系统等技术手段进行访问控制。

·权限限制

权限限制访问控制是指基于最小特权原则、最小泄露原则、多级安全策略来限制用户对数据或资源的访问。常见的权限限制访问控制方式，包括：访问控制表、访问控制矩阵、访问控制能力列表、访问控制安全标签列表等，例如，通过对比用户的安全级别和客体资源的安全级别（绝密、秘密、机密、限制以及无级别）来判断用户是否有权限可以进行访问；对用户进行角色划分，并授予管理用户所需的最小权限，实现管理用户的权限分离；对系统资源的访问是通过访问控制列表加以控制的，即当用户试图访问资源或者数据时，系统会控制用户对有安全标记资源的访问。

·端口开放访问控制

服务器传输数据过程，除了需要目标IP地址外，还需要开放一些服务端口。通

过系统的端口，能够使运行不同操作系统的计算机应用进程互相通讯。端口分为公认的默认端口和动态端口。默认端口是用于明确某种服务的协议，例如默认情况2端口是分配给FTP服务，25端口分配给SMTP服务，80端口分配给HTTP服务；动态端口则是用于动态分配给一些系统进程或应用程序。应用服务器应根据提供服务的需求，有限开放对应端口，限制不必要的端口开放，从而有效限制数据传输泄密的风险。

4.5 重点行业领域数据传输安全

·数字政府数据传输安全

国务院于2022年6月6日发布的《国务院关于加强数字政府建设的指导意见》强调了数字政府是数字中国的重要组成部分之一，是顺应历史趋势的必然选择以及战略选择。数字政府以数据为关键驱动，提供宏观层面更精准、更有效、更实时的决策分析支撑。数字政府的建设，是政务管理的数据化转型，涉及到各部门协同组织关系变革，重点在于数据管理部门，目前不少省份组建大数据局，负责承建省市的政务云系统及政务网络建设。政务网作为独立的专网环境，大量的政务数据高频流通，涉及到民生各个方面的数据，如人口信息、家庭信息、婚姻信息、学籍管理、交通管理、资产管理等。因此，政务专网的数据传输安全、端口安全尤其重要。

数字政府安全保障体系必须采用严格的数据安全技术措施来保证数据在传输过程的保密性，如通过数据加密、去标识化、数据脱敏、安全通道等技术措施。在数字政府网络区域边界进行有效的访问控制管理，删除多余或无效的访问控制规则，具备根据回话状态信息识别数据流进行有效控制管理。网络节点有效监控网络攻击行为，恶意代码进行检测和清除，维护恶意代码防护机制，部署安全审计设备。针对跨网数据传输，应建立从业务专网传输可开放且非涉密的数据至电子政务网的高效传输机制，并通过数据安全通道等技术措施来保障数据传输过程中的安全性，进一步构建协同高效的政府数字化履职能力体系。

·金融行业数据传输安全

中国人民银行于2021年2月9日发布了《金融数据传输能力发展指南》，从数据保护和金融数据分类指南方面规范了数据传输安全目标。针对不同级别的数据应具备不同的安全保护能力，而相对应的数据传输策略也会有所不同。数据分类管理依据影响对象和影响程度这两个标准将安全级别从低到高分为5个等级。针对客户体量大，即客户质量高以及客户数量多，涉及客户资金量多、行业多，数据传输规模大，客户敏感信息数量多、比重大的情况，数据等级宜从高确定，且应具备更高级别的安全保护能力，其中数据传输策略也应更完善。

金融行业应建立数据传输安全监控机制，覆盖数据全生命周期，对数据传输安全策略进行监控，并适时优化调整来保证数据传输的可用性以及数据传输安全策略的有效性。基于实际的工作重点建立数据传输安全策略，采用数据加密、去标识化、安全通道等技术措施。如：当遇到公共网络传输的场景时，应采用安全通道、数据加密、去标识化等安全技术措施进行传输，保障数据传输过程中数据的保密性和安全性；对于支付账号等敏感信息，应根据《中国金融移动支付支付标识化技术规范》的规定，采用使用支付标记化技术等安全传输技术控制措施来进行脱敏处理，来保证数据传输的保密性；对于高级别数据要通过数据加密（加密方法或者加密协议）、过滤等安全传输保障手段来保证数据的保密性和安全性等。

·车联网行业数据传输安全

车联网（IOV）是新一代网络通信技术与汽车、电子、道路交通运输等领域深度融合的新兴产业形态，是物联网在智能交通系统（ITS）领域的延伸，是以车内网、车际网和车载移动互联网为基础，利用先进的传感技术及车载计算平台技术，通过汽车收集、处理大量信息，并按照约定的通信协议和数据交互标准，实现V2X（X包括车、路、行人、通信、服务平台）无线通讯和信息交换的大系统网络，以支持智能交通管理控制、车辆智能化控制和智能动态信息服务等应用。聚焦自动驾驶数据传输方面的安全风险，重点关注传输节点和传输通信过程风险。

传输节点恶意攻击风险：在车-车通信中，攻击车辆可以冒充正常行驶车辆，向目标车辆发送伪造数据；在车-设施通信中，攻击者可以安放恶意攻击路侧设施，窃取车辆行驶数据或向车辆发送错误交通数据干扰车辆行驶；在车-云通信中，攻击者可以伪造传感器节点或者云端接口，伪造和篡改自动驾驶数据；在车内通信中，攻击者可以设置攻击车辆电子控制单元（ECU）节点，接收指令数据后，对数据进行重写、伪造和篡改，再发送给车内其他ECU，使自动驾驶汽车做出错误的执行操作。

数据传输通信风险：自动驾驶汽车参与车联网活动需要通过数据通信完成与其他实体的信息交互。数据通信包括车内网通信、车际网通信和车载移动互联网通信三种情况。车内网通信主要指车载CAN总线或车载以太网通信，目前车内网通信安全防护机制还比较薄弱，CAN报文采用明文广播传输，易被篡改或伪造，CAN协议则易被破解，还有可能发生通信总线被攻击消息阻塞从而导致总线通信失效风险，一旦发生以上情况，自动驾驶数据采集、智能决策等都会受到影响，从而带来安全驾驶的风险。车际网通信主要指车辆通过蓝牙、WIFI、DSRC、C-V2X等与其他车辆、路侧设施等进行的数据通信，在没有安全防护的信道中，数据通信会面临被窃听或遭受中间人攻击的风险。在V2V通信中，自动驾驶车辆会广播本车的坐标信息，在未加密的情况下，攻击车辆可以窃取大量地理信息数据，存在个人隐私数据甚至国家秘密泄露的风险。车载移动互联网通信过程中，一般会利用数字证书机制加强数据通信的安全保障，否则，也会出现数据被监听、被篡改等安全风险。

2021年多份涉及智能网联汽车网络信息安全的文件密集出台，其中，《关于加强智能网联汽车生产企业及产品准入管理的意见》中明确提出了准入测试要求，《汽车数据安全管理若干规定(试行)》界定了“汽车数据处理者”和“重要数据”类型等内容；工信部《关于加强车联网网络安全和数据安全工作的通知》，要求加强车联网网络安全和数据安全管理工作；2022年3月7日工信部印发了《车联网网络安全标准体系建设指南》，智能网联汽车的安全标准建设更趋于体系化。

五、数字政府应用场景

随着数字政府建设不断深入，政务数据规模快速增长，海量数据的收集、存储、使用、加工、传输、提供、公开，增加了数字政府网络安全防护难度，亟需构建数字政府安全屏障。

5.1 数字政府建设总体情况

数字政府是全面数字化发展的基础性、先导性工程，在促进数字经济、建设数字社会、完善数字生态中起到关键的引领作用。加强数字政府建设是创新政府治理理念和方式的重要举措，对加快转变政府职能，建设法治政府、廉洁政府、服务型政府意义重大。近年来，我国数字政府建设取得显著成效，以数字化促改革、以数字化助决策、以数字化提服务的理念不断深入人心，一体化政务服务和监管效能大幅度提升，“一网通办”、“最多跑一次”、“一网统管”、“一网协同”等服务管理新模式广泛普及，数字营商环境持续优化，在线政务服务水平跃居全球领先行列。

数字政府建设顶层设计不断加强。《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》明确提出加快建设数字经济、数字社会、数字政府，以数字化转型整体驱动生产方式、生活方式和治理方式变革。随后广东、浙江、上海、江苏等主要省市纷纷发布数字政府建设相关的专项规划，积极加快推进数字政府建设。

数字政府建设体制机制逐步完善。全国各省市陆续成立数字政府建设领导小组和省级大数据管理局，加快构建体系化规范化的数字政府管理机构，统筹推进数字政府建设。广东省在全国率先推行首席数据官(CDO) 制度，并遴选6 个省级政府部门、10 个地市级政府等同步开展试点，明确将“首席数据官”列为数字政府建设的第一负责人，构建了贯穿省、市、县三级的数字政府专人专岗梯度管理体系，为数字政府岗位责任制一体化部署做出了重大贡献。

数字政府建设协同合作持续深入。各省市积极推动数字政府建设优势互补、多元协作。上海市发布《上海市公共数据开放暂行办法》，建立公共数据开放的长效机制，优化公共数据开放平台建设，打造公共数据多元开放系统，在医疗、交通、文旅等领域广泛征集公共数据开放与开发利用试点项目，推动政企数据融合，引导数据挖掘赋能行业应用创新，合作形式更加多元，落地举措更加开放。

数字政府建设亟需构建安全屏障。随着数字政府建设不断深入，政务数据规模快速增长，海量数据的收集、存储、使用、加工、传输、提供、公开，增加了数字政府网络安全防护难度。同时，受内外部多重因素影响，数字政府面临的网络安全威胁日益凸显，网络攻击形势愈加明显，网络安全形势愈加严峻复杂，亟需构建数字政府的安全屏障。

5.2 数字政府建设中数据传输场景及解决方案

数字政府建设数据传输安全应用场景主要分为面向政务服务/政务公开、面向智慧城市、面向部门协同、面向内部管理的数据传输，各应用场景的主体、客体、行为和特点如表所示。

序号	应用场景	主体	客体	行为	特点
1	面向政务服务/政务公开的数据传输	企业或个人、相关行政机关相关部门	企业数据和个人数据/政务公开信息	数据从政务服务客户端到政务服务服务器的双向传输	发送方/接收方请求量大且分布广泛
2	面向智慧城市的数据传输	数据源、相关业务部门	生态环境和社会治理相关的数据	数据通过智能感知设备进行采集，再传输到网关，通过网关传输到智能感知平台	发送方数量大、发送方种类多，发送方覆盖范围广

序号	应用场景	主体	客体	行为	特点
3	面向部门协同的数据传输	业务部门	业务数据	数据从业务部门传输给政务数据管理中心，再传输到需要数据的业务部门；数据直接从业务部门直接传输到需要数据的业务部门	主体数量较为有限，范围相对固定
4	面向内部管理的数据传输	政府部门负责相关工作的员工、相关业务部门	内部管理涉及的数据	数据从客户端传输到业务部门的服务器	主体数量有限，范围固定

5.2.1 面向政务服务 / 政务公开的数据传输

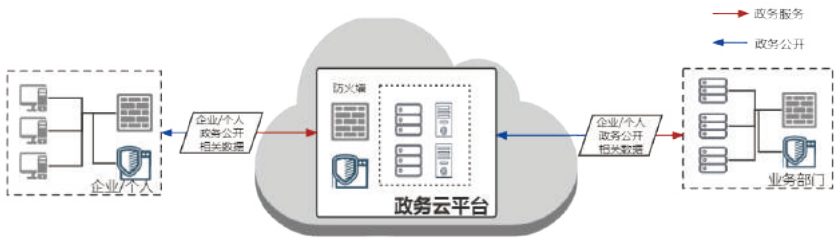
(1) 应用场景数据传输需求

政务服务是指政府相关部门及事业单位通过政务服务平台，为企业、个人等提供的许可、确认、裁决、奖励、处罚等行政服务。发送方为企业或个人，接收方为相关业务部门，传输的数据为法人办事、个人办事过程中涉及的企业数据和个人数据，具有发送方请求量大且分布广泛的特点。法人或个人通过政务服务客户端将数据传输到相关业务部门的服务器，服务器将处理结果反馈。

政务公开是指行政机关在履行职责过程中制作或者获取的，以一定形式记录、保存的信息，及时、准确地公开发布。发送方为行政机关相关部门，接收方为企业或个人，传输的数据为政务公开信息，具有接收方请求量大且分布广泛的特点。行政机关相关部门通过政务服务服务器将数据传输到政务服务客户端，企业或个人可通过政务服务客户端查询和浏览。

(2) 应用场景数据传输安全风险

• 业务流程图



• 主要风险点

- 恶意客户端接入
- 数据从客户端传输到服务器的过程中发生泄漏、窃取、篡改等
- 恶意服务器调用

(3) 应用场景数据传输安全解决方案

- 恶意客户端接入、恶意服务器调用

客户端和服务器之间的数据传输通常使用客户端向服务器上传数据和服务器从客户端拉取数据两种方式，当客户端或服务器被恶意篡改或伪造时，会导致传输的数据发生泄漏、窃取、篡改等。

管理方面，可建立传输主体安全管理规范，明确身份鉴别、签名验签、数据传输接口等安全要求，建立密钥安全管理规范，明确密钥生成、分发、存取、更新、备份和销毁的流程和要求，建立权限安全管理规范，明确权限的申请、修改等管理要求。

技术方面，可采用客户端准入控制等方式，降低未授权客户端接入风险，通过客户端加壳、完整性校验、密钥双向校验等技术措施，降低客户端和服务器被恶

意篡改或伪造的风险，优化权限策略，加强权限收敛，减少越权访问的风险。

- 数据从客户端传输到服务器的过程中发生泄漏、窃取、篡改等

管理方面，可建立数据传输安全管理规范，明确传输通道加密、数据内容加密等安全要求，建立传输缓存清除机制。

技术方面，可对传输通道和数据内容进行加密，并通过对加密算法、密钥强度进行优化和升级，提升数据传输过程中的安全性，在数据传输不完整或传输完成时清除缓存和历史缓存数据。

5.2.2 面向智慧城市的数据传输

（1）应用场景数据传输需求

智慧城市依托智能感知网络采集气象、环境、噪声、火灾、治安等数据，为智慧城市生态环境和社会治理提供数据支撑。发送方为生态环境和社会治理数据源，接收方为生态环境、公安等相关业务部门，传输的数据为涉及生态环境和社会治理相关的数据，具有发送方数量大、发送方种类多，发送方覆盖范围广等特点。数据通过气象监测设备、环境监测设备、噪声监控设备、火灾监测设备、治安监测设备等智能感知设备进行采集，再通过有线或无线的方式传输到网关，通过网关传输到相关业务部门的智能感知平台。

（2）应用场景数据传输安全风险

- **业务流程图**

• 主要风险点

- 恶意智能感知设备接入网关
- 智能感知设备接入到网关的传输通道和数据内容受到破坏
- 恶意智能感知平台接入网关
- 智能感知平台接入到网关的传输通道和数据内容受到破坏

（3）应用场景数据传输安全解决方案

- 恶意智能感知设备/智能感知平台接入网关

智能感知设备和智能感知平台的数据传输面临更多更强的安全风险和威胁，特别是智能感知设备，更容易遭到捕获、攻击时，造成恶意接入，从而破坏数据传输的安全性。

管理方面，可建立传输主体安全管理规范，明确身份鉴别、签名验签、数据传输接口等安全要求，建立密钥安全管理规范，明确密钥生成、分发、存取、更新、备份和销毁的流程和要求，建立权限安全管理规范，明确权限的申请、修改等管理要求；对于智能感知设备，建立入侵检测机制，及时对识别异常设备，加强智能感知设备账号管理，及时停用长时间未使用的账号，强化管理账号和口令安全，禁止使用弱口令，建立安全管理基线。

技术方面，可通过完整性校验、密钥双向校验等技术措施，降低服务器和客户端被恶意篡改或伪造的风险，优化权限策略，加强权限收敛，减少越权访问的风险；对于智能感知设备，使用适用于智能感知设备的入侵检测技术，实现入侵的监测、跟踪和响应。

- 数据传输过程中传输通道和数据内容受到破坏

管理方面，可建立适用于智能感知设备、智能感知平台有线或无线传输的数据传输安全管理规范，明确传输通道加密、数据内容加密等安全要求。

技术方面，可使用适用于智能感知设备、智能感知平台有线或无线传输的方式，对传输通道和数据内容进行加密，并通过对加密算法、密钥强度进行优化和升级，提升数据传输过程中的安全性。

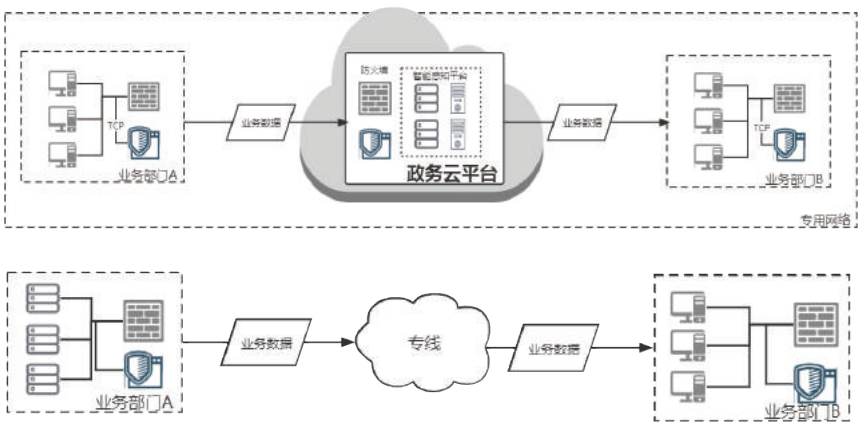
5.2.3 面向部门协同的数据传输

（1）应用场景数据传输需求

部门协同是指通过部门之间业务数据整合共享，推动跨层级、跨地域、跨部门、跨系统、跨业务的纵深联动、高效协同。发送方为提供数据的业务部门，接收方为需要数据的业务部门。传输的数据为部门之间整合共享的业务数据，具有主体数量较为有限，范围相对固定的特点。部门之间业务数据传输有两种方式，一种是提供数据的业务部门把传输给政务数据管理部门，再通过政务数据管理中心传输给需要数据的业务部门，另一种是提供数据的业务部门直接把数据传输给需要数据的业务部门。

（2）应用场景数据传输安全风险

- 业务流程图



• 主要风险点

- 传输通道受到破坏

- 传输内容发生泄漏、窃取、篡改等

（3）应用场景数据传输安全解决方案

- 传输通道受到破坏

面向部门协同办公的主体数量较为有限，范围相对固定，且传输的多为业务数据，可根据业务数据采用专用网络或点对点专线进行传输。

管理方面，可建立专用网络和专线安全管理规范，明确专用网络和专线的安全管理要求。

技术方面，可通过部署防火墙等安全设备，应对外部攻击，做好内部网络的漏洞扫描、主动防御等，保证传输通道的安全，并对传输通道进行加密。

- 传输内容发生泄漏、窃取、篡改等

管理方面，可建立数据传输安全管理规范，明确数据内容加密等安全要求，根据需要制定数据脱敏规则，定期对数据传输安全性和可靠性进行检查和评估。

技术方面，可对数据内容进行加密，并通过对加密算法、密钥强度进行优化和升级，提升数据传输过程中的安全性，并根据需要对业务数据进行脱敏处理。

5.2.4 面向内部管理的数据传输

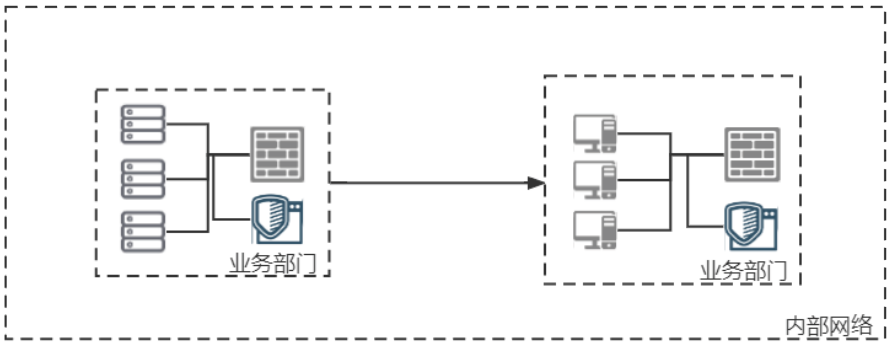
（1）应用场景数据传输需求

内部管理是指通过信息化的方式实现政府部门的内部管理，主要包括办公自

动化系统、人事管理系统、财务管理系统等。发送方为政府部门负责相关工作的员工，接收方为相关业务部门。传输的数据为内部管理涉及的办公数据、人事数据、财务数据等，具有主体数量有限，范围固定的特点。负责相关工作的员工将数据通过客户端传输到业务部门的服务器，服务器将处理结果反馈。

（2）应用场景数据传输安全风险

- **业务流程图**



- **主要风险点**

  - 传输通道受到破坏
  - 传输内容发生泄漏、窃取、篡改等

（3）应用场景数据传输安全解决方案

  - 传输通道受到破坏

面内部管理的主体数量有限，范围固定，且传输的多位内部数据，可采用内部网络进行传输。

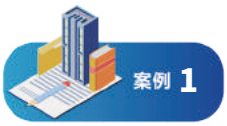
管理方面，可建立内部网络安全管理规范，明确内部网络的安全管理要求。

技术方面，可通过部署防火墙等安全设备，应对外部攻击，做好内部网络的漏洞扫描、主动防御等，做好内部网络和外部网络的安全隔离，保证传输通道的安全，并对传输通道进行加密。

- 传输内容发生泄漏、窃取、篡改等

管理方面，可建立数据传输安全管理规范，明确数据内容加密等安全要求，做好数据从内部向外部传输的管理要求，根据需要制定数据脱敏规则。

技术方面，可对数据内容进行加密，并通过对加密算法、密钥强度进行优化和升级，提升数据传输过程中的安全性，做好数据从内部向外部传输的技术限制，并根据需要对业务数据进行脱敏处理。



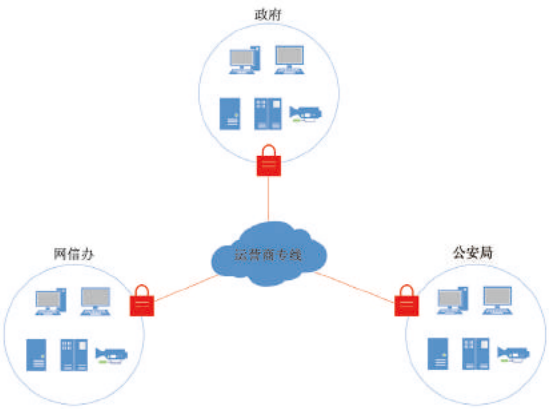
数字政府建设数据传输安全应用场景 1

需求分析

主体: 发送方是某地网信办，接收方是某地公安局及相关政府监管部门;

客体: 执法音频视频数据，多部门联动的视频会议数据，以及交换共享的相关数据;

行为: 通过租用运营商提供的专用线路来建立网信与公安、网信与政法、网信与通管局的链路数据通信。



解决方案

1、通过隐蔽自身设备及操作系统，隐蔽网络接口与隐蔽设备部署位置、隐蔽保护后端的网络资产设备的业务端口和漏洞不被探测或扫描发现，确保“安全堡垒”自身隐蔽、安全。

2、创新采用网络安全技术、数据安全技术、防绕过技术、安全隔离等技术，有效防止勒索攻击、 SQL注入攻击、CGI访问攻击、IIS服务器攻击、 远程注入等“绕过攻击”，确保信息网内安全。

3、采用国密SM4加密算法，对数据进行随机加密无特征化处理，防止被劫持数据还原、通信中被恶意引流、无感知会话劫持等风险；采用创新的数据压缩+数据混淆+数据加密技术，以及数据流进行双向隔离技术，实现信息在传输中无特征、无感知、无法被网络外部侦测、过滤、劫持和数据还原，确保信息传输安全。

4、通过创新的“微隔离”技术，根据不同需要进行各种分级、分区匹配和控制，实施数据双向隔离，实现网络和数据在不同横向部门间的加密通信与多重加密；进行单个会话或多网段主机之间的微隔离与控制，实现对同一台主机、不同应用、不同业务间灵活的微隔离控制，保障信息在不同的范围内受控与交互。

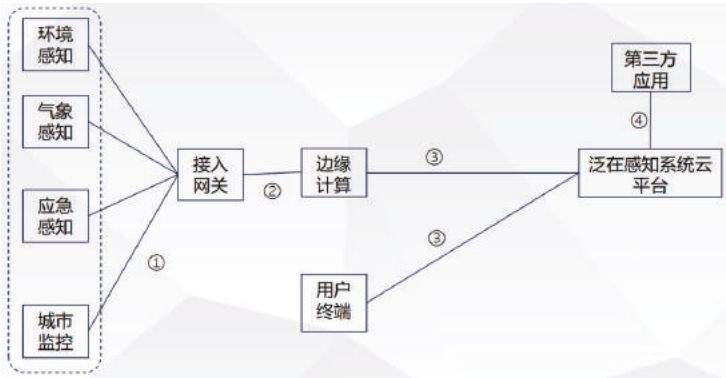
数字政府建设数据传输安全应用场景 2

需求分析

主体：数据发送方是各种感知设备，数据接收方为感知平台；

客体：涉及环境、气象、应急和城市监控等方面的数据；

行为：感知设备将采集到的数据汇聚到网关，网关通过光纤将数据传输到边缘云服务器，或云平台，云平台将数据对接各应用。



解决方案

1、定期对感知设备进行巡检，排查设备非法接入；对每个感知设备，生成设备指纹，接入网络时进行设备认证，并且只有通过认证的设备才能接入网络。

2、定期对边缘计算物理防护设备进行巡检，制定进出边缘计算设备钥匙管理制度和人员信息安全培训；登录边缘计算设备采用Ukey进行身份鉴别，并且根据用户角色分配相关权限，对操作进行审计以及审计日志防篡改。

3、制定信息安全管理制度，结合法律法规，对违反信息安全给予相关处罚，加强用户信息安全培训，减少主动违反的动机。登录边缘计算设备采用Ukey进行身份鉴别，并且根据用户角色分配相关权限，对操作进行审计以及审计日志防篡改。

4、加强对租用网络供应商的管理，压实其责任；建立VPN通道，保证传输数据的机密性、完整性。

5、从人员、操作和敏感信息保护角度制定完善的管理制度，并定期多运维人员开展培训，避免内部人员引发信息安全事件；对重要数据，敏感数据使用密码机等设备进行机密性、完整性保护，对于关键操作使用签名验签服务器进行抗抵赖处理。

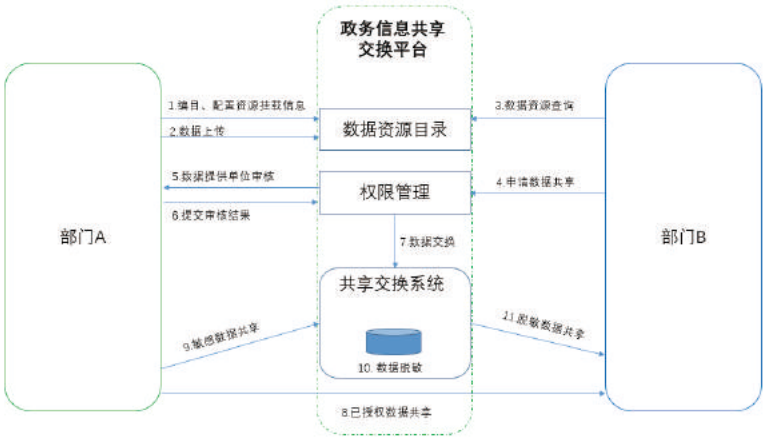
数字政府建设数据传输安全应用场景 3

需求分析

主体：发送方为数据共享平台的维护部门，接收方为资源数据的请求方/申请方；

客体：实际的数据需求；

行为：直通模式，代理模式，服务模式。



解决方案

1、为确保数据传输通道安全性，需采用加密的传输通道/协议（专网、专线、IPsec、Https等）；若传输的数据内容涉及敏感个人信息及重要数据的，还需对传输的数据内容进行脱敏处理，若因业务所需，则对传输的数据内容进行加密，并对数据进行签名，保障数据的机密性、完整性。

2、为确保数据传输通道可靠性，传输前需对传输数据的两端进行身份鉴别，在数据传输通道边界部署安全设备，随时监控数据过程中出现异常行为时，能进行有效阻断；在数据传输通道的关键节点部署冗余的网络设备及备用传输通道，保障数据传输出现故障时，有效保障数据传输服务。

3、数据交换过程中，需对整个交换事务进行有效记录，记录的信息包含但不限于：数据传输的身份鉴别信息、数据传输过程信息（IP，数据长度，传输时间等）、异常记录。

4、需建立有效的访问控制及数据行为监督的机制，确保数据传输双方的访问权限分配合理、合规，定期对数据交换的平台传输通道进行检查与评估，定期对数据行为日志进行分析，确保数据传输安全、可靠。

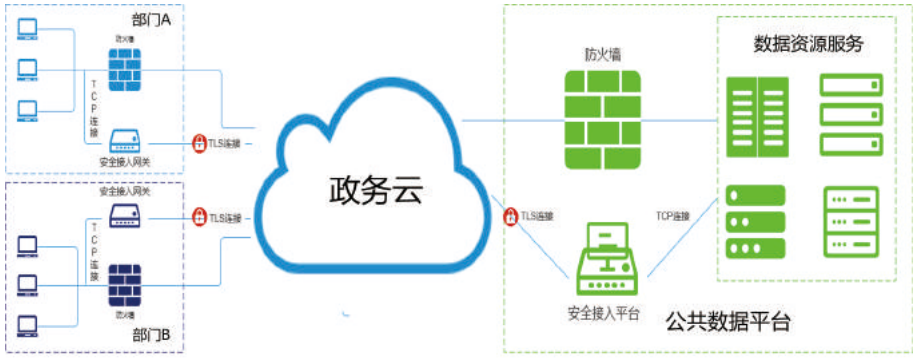
数字政府建设数据传输安全应用场景 4

需求分析

主体：发送方为某市大数据局，接收方为某市各政府部门；

客体：涉及业务系统资产地图中的数据；

行为：采用TLS保证通讯双方的信息安全，依赖TCP传输层来传输和接收数据，采用SM2、SM4进行链路数据加密，利用特有应答纠错机制保证数据包有序、完整到达。



解决方案

1、大数据局需要将对应的服务映射到政务外网上，通过政务外网进行安全访问，因部分系统地址不方便对外公开，因此需要通过链路加密及代理地址等进行安全访问，访问服务器应用/系统时，需要实时监控资源访问流量、自动记录相关日志，如发现有可疑链路访问，则需要进行中断会话，以此对系统地址进行伪装/代理访问，减少来自内外部的威胁。

2、通过管理办法及网络技术将大数据局的网络与政务云的专网连接，同时隔绝外网的访问。

3、通过客户端进行代理端口访问，一是针对身份的多因素的认证，自动判别登录主体的合法性；二是对用户行为信息进行记录管理，提供追溯分析；三是通过敏感SQL管理、SQL注入防护和数据库漏洞防护等手段实现数据防勒索。

4、客户端和服务器之间可自定义增加脱敏规则，提供SHA1加密、MD5加密、AES加密、RSA加密、随机映射、固定映射、替换、截断、截取，以及保留、取整、范围内浮动、比例内浮动等各种脱敏算法，支持分段配置不同的脱敏规则；客户端和服务器之间为国产加密算法（SM2、SM4）进行链路数据加密，任何途径抓取的流量包/数据都为脱敏加密。

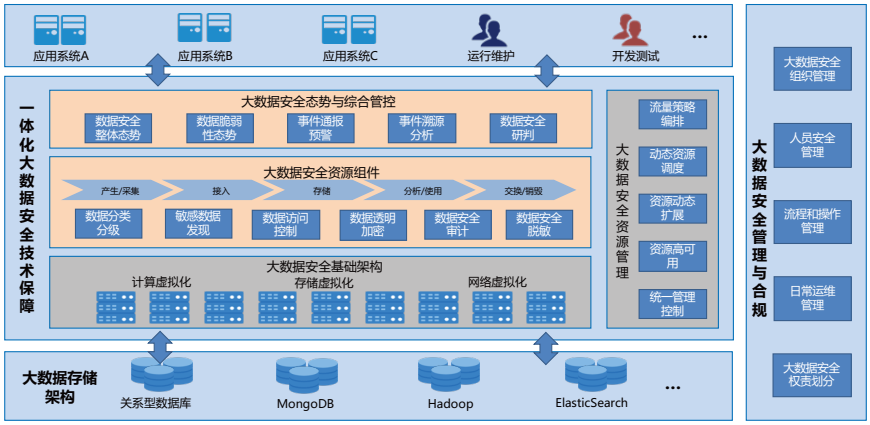
数字政府建设数据传输安全应用场景 5

需求分析

主体：发送方为某地政数局，接收方为某地委办局；

客体：社保、财政等相关数据；

行为：政数局和委办局之间进行数据传输；政数局和委办局在政务大数据中心进行上传和下载数据。



解决方案

1、利用LDAP/AD、Radius、第三方CA、自建CA、短信认证、硬件特征码、动态令牌多种安全认证方式并结合可信安全接入网关，通过多因素组合认证最大限度地保证了接入通信双方的合法性；加强数据安全管理的账号权限管理及审批，关注组织内部不同账号类型对生产数据库进行操作的权限管理及授权审批规则，有效防范内部人员恶意窃取、泄漏数据的风险。

2、针对政务数据资产和信息系统管理流程，建立数据资产和信息系统的安全管理规范，明确安全管理目标和安全原则，定义数据资产和信息系统的管理者和所应承担的职责；构建业务数据资产清单，建立数据资产和信息系统的分类分级方法和操作指南，明确分类分级的变更审批流程；依据数据主体分级要求建立相应的标记策略、访问控制、数据加解密、数据脱敏等安全机制和管控措施。

3、建立数据共享安全管理制度，开展数据共享活动前，对数据接受方的背景、资质进行审查；二是检验数据接受方的数据安全保护能力，保障数据共享后的安全水平不降低；签订安全协议或在合同中设置安全条款，明确双方安全责任。

数字政府建设数据传输安全应用场景 6

需求分析

主体: 发送方和接收方均为应急指挥系统省市县三级视频会议节点;

客体: 应急指挥视频调度中的音视频实时数据流;

行为: 采用IPSec协议保证网络中各节点的接入认证和传输安全; 采用SM2算法进行密钥协商, 采用SM4算法进行链路加密, 采用SM3+MAC对网络报文进行完整性保护。

需求分析

1、在省级单位与地市级单位的专用线路中, 通过直连方式部署吞吐率为13Gbps的万兆型主干路IPsec VPN安全网关, 实现大数据量、低延时的数据安全传输, 确保数据传输的机密性、完整性。

2、在区县级单位侧部署千兆型IPsec VPN安全网关, 与地市级单位侧进行直连, 实现区县级单位与地市级单位数据传输的机密性、完整性。

3、在省级节点部署视频调度系统传输加密管理平台, 为各节点入网设备统一签发数字证书, 基于SM2数字证书认证机制, 实现各节点入网设备的身份认证。

4、通过视频调度系统传输加密管理平台对各节点入网设备统一下发通信策略, 统一密码算法和隧道协议, 保证各节点之间通信协议的一致性。

5、采用SM2+SM4+SM3+ESP隧道模式, 在各节点之间, 构建安全传输通道, 组建虚拟专用网, 各节点之间通信链路采用SM4算法进行加密, 采用SM3+MAC保证通信报文的完整性。

6、音视频数据流通过IPSec加密隧道进行传输, 保证数据流的完整性和机密性, 防止数据泄露和被恶意篡改。

六、数字金融应用场景

金融数据泄露、滥用、篡改等安全威胁影响重大，涉及用户个人隐私和企业商业机密，关乎国家安全和社会稳定，数字金融安全能力建设重要性凸显。

6.1 数字金融建设总体情况

数字金融是通过互联网及信息技术手段与传统金融服务业态相结合的新一代金融服务，依托于大数据、云计算、人工智能、区块链等一系列技术创新，为用户提供支付清算、借贷融资、财富管理、零售银行、保险、交易结算等金融产品和服务。近年来，随着数字经济创新发展，数字技术与金融深度融合，我国数字金融建设持续推进，为促进企业和产业数字化转型升级的提供了重要支撑。

数字金融新业态新应用不断涌现。目前数字金融的应用范围涵盖数字支付、数字货币、线上信贷、数字证券、智能理财、数字保险等新型业务形态，主要参与机构包括银行、保险、证券、资产管理等金融机构，以及互联网平台企业。金融服务正从单点服务向场景服务转变，从单向服务向赋能服务转化，开放银行平台等金融场景生态建设持续推进。

数字金融服务覆盖范围扩展迅速。我国数字金融在立足机会平等要求和商业可持续原则基础上，不断突破金融服务触达范围和辐射半径，为有金融服务需求的社会各阶层和群体提供适当、有效的金融服务，让数字金融发展成果惠及更多人民群众，尤其是小微企业、农民、城镇低收入人群等弱势群体，为企业帮扶、脱贫攻坚作出了巨大贡献，助力共同富裕奋斗目标的实现。

数字金融规范化建设稳步推进。2022年，《关于银行业保险业数字化转型的指导意见》《金融科技发展规划(2022-2025年)》等重要文件的先后印发，对金融机构的数字化转型和安全发展提出了明确的目标和要求，《金融数据安全数据安全分级指南》等标准也对数据安全性被破坏的情况下，造成的影响程度以及影响对象进行了划分，法律法规和标准体系逐步完善。

数字金融安全重要性日益凸显。金融数据随着数字经济的创新发展呈现爆发式增长，数据采集渠道和维度多元化，数据价值密度高、应用价值大的特点愈发突出。金融数据的泄露、滥用、篡改等安全威胁影响重大，涉及用户个人隐

私和企业商业机密，关乎国家安全和社会稳定。加强金融数据安全能力建设既是金融机构发展的内生需求，也是行业强监管的客观要求。

6.2 数字金融建设中数据传输场景及解决方案

数字金融数据传输安全应用场景主要分为面向内部协同、面向金融服务、面向外部合作和面向跨境流动的数据传输，各应用场景的主体、客体、行为和特点如表所示。

序号	应用场景	主体	客体	行为	特点
1	面向内部协同的数据传输	金融机构及各分、子公司内部人员	机构信息、金融信息、经营数据、分析报告、系统及应用日志等数据	在同一数据中心的情况下，通常采用内部网络进行传输；在不同数据中心的情况下，通常采用 VPN 或基于专线技术的机构内骨干网进行数据传输。	传输主体数量较为有限，范围相对固定
2	面向金融服务的数据传输	金融客户、金融机构相关业务部门	客户金融信息	金融客户通过客户端访问金融服务平台，进行业务办理，客户端反馈业务结果	发送方请求量大、分布范围广泛
3	面向外部合作的数据传输	金融机构与其他数据供应方、业务合作机构、政府及监管机构等外部机构	金融信息、风控信息、业务信息和公业务信息等数据	机构间通常采用机构专线或 VPN 进行数据传输	主体数量较为有限，范围相对固定

序号	应用场景	主体	客体	行为	特点
4	面向跨境流动的数据传输	金融机构、海外分支机构或总部、其他境外金融机构、第三方数据处理服务商、境外监管机构或行政与司法部门等	个人金融信息、企业金融信息以及金融机构运营的业务数据等在内的金融数据	金融机构将存储在境内的相关金融信息，通过跨境传输平台传输至境外，或境外的机构、组织、个人通过访问跨境业务平台，进行业务办理	合规评估复杂，境外屡责落实难

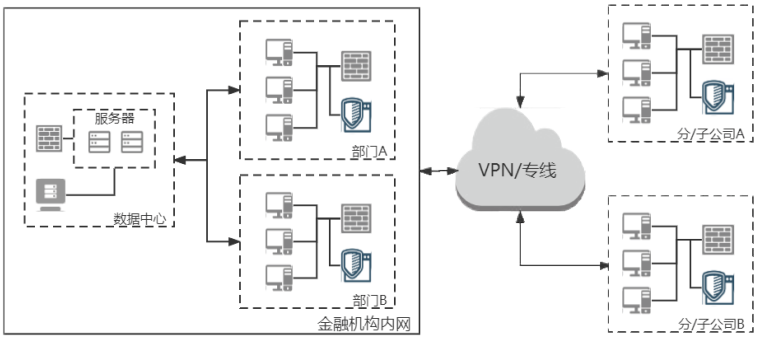
6.2.1 面向内部协同的数据传输

（1）应用场景数据传输需求

内部协同是通过金融机构及其各分、子公司的数据整合共享，实现机构内部跨层级、跨地域、跨部门、跨系统的高效业务协同。数据发送方和接收方均为金融机构及各分、子公司内部人员，传输的数据为金融机构内部整合共享的业务数据、金融数据等，具有主体数量较为有限，范围相对固定的特点。金融机构的业务协同在同一数据中心的情况下，通常采用内部网络进行传输，数据发送方通过数据中心将数据传输给接收方；在不同数据中心的情况下，如金融机构与其分、子公司之间，通常采用VPN或基于专线技术的机构内骨干网进行数据传输。

（2）应用场景数据传输安全风险

- 业务流程图



• 主要风险点

- 数据传输通道受到破坏
- 数据传输过程中发生泄露、窃取、篡改等

（3）应用场景数据传输安全解决方案

- 数据传输通道受到破坏

管理方面，可建立内部网络和专线安全管理规范，明确内部网络和专线的安全管理要求。

技术方面，可通过部署防火墙等安全设备，应对外部攻击，同时做好内部网络的漏洞扫描、主动防御等，不同网络区域或者安全域之间应进行安全隔离和访问控制，并对传输通道进行加密，保证传输通道的安全。

- 数据传输过程中发生泄露、窃取、篡改等

管理方面，可建立金融信息保护制度体系及保护规范工作流程，明确工作职责。可对金融信息进行分级分类，不同类别、安全级别的金融信息，采用不同的管理措施及传输方式。可留存数据操作行为日志，针对日志进行事后审计分析，识

别并告警可疑行为。

技术方面，终端应采取准入控制、终端鉴别等技术措施，防止非法或未授权终端接入内部网络。同时可对数据内容进行加密，并通过对加密算法、密钥强度进行优化和升级，提升数据传输过程中的安全性，并根据需要对业务数据进行脱敏处理。

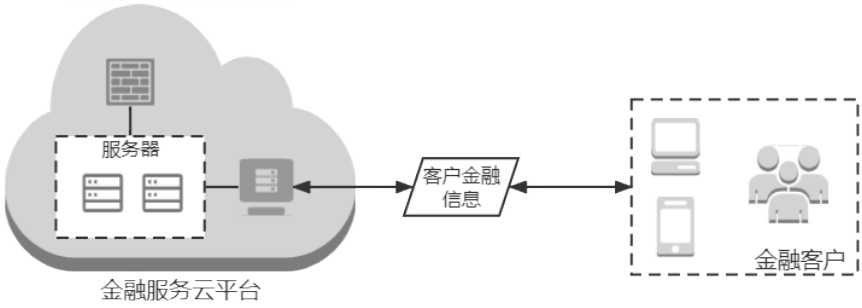
6.2.2 面向金融服务的数据传输

（1）应用场景数据传输需求

金融服务是指金融机构通过金融服务平台，为金融客户提供融资、投资、储蓄、信贷、结算、证券买卖、商业保险和金融信息咨询等服务。发送方为金融客户，接收方为金融机构相关业务部门，传输的数据为账户信息、金融交易信息、身份信息、财产信息、借贷信息等客户金融数据，传输具有及时性，且发送方具有请求量大、分布范围广泛的特点。金融机构与金融客户数据传输主要采用有线互联网、移动互联网、第三方互联网应用、无线互联网等方式，金融客户可通过客户端访问金融服务平台，进行业务办理，客户端反馈业务结果。

（2）应用场景数据传输安全风险

- **业务流程图**



• 主要风险点

- 恶意服务器接入
- 恶意客户端调用
- 数据传输过程中发生泄漏、窃取、篡改等

（3）应用场景数据传输安全解决方案

有线互联网、移动互联网、第三方互联网应用、无线互联网等网络容易被攻击者利用传输的漏洞、布网的缺陷或简陋配置窃取传输信息。

- 恶意客户端接入、恶意服务器调用

管理方面，应根据数据的不同安全级别，制定和明确数据访问控制过程中的相关管理措施，建立金融信息保护制度体系及保护规范工作流程，明确工作职责。

技术方面，应对传输双方身份采用数字签名、时间戳等方式进行鉴别和认证。终端应采取准入控制、终端鉴别等技术措施，防止非法或未授权终端接入。应建立日常数据泄露、数据篡改、数据窃取、数据非法使用的风险监控机制，主动预防、发现和终止数据泄露异常行为。在数据传输完成后或不完整时及时清除历史传输缓存数据。

- 数据传输过程中发生泄漏、窃取、篡改等

管理方面，应建立金融信息保护组织架构，明确在提供金融产品和服务的过程中知悉金融信息的岗位，并针对相关岗位明确其金融信息安全管理责任与保密责任。

技术方面，应按照行业标准对金融信息分类，不同类别使用不同的技术手

段保证金融信息传输安全。可采用防火墙、入侵检测等安全技术或设备，确保数据传输网络的安全性；使用加密通道或数据加密的方式进行传输，同时建立对通道安全配置、密码算法配置、密钥管理等保护措施的管理和监控机制。

6.2.3 面向外部合作的数据传输

（1）应用场景数据传输需求

外部合作是指金融机构与其他数据供应方、业务合作机构、政府及监管机构等外部机构之间的合作，传输的数据为金融信息、风控信息、业务信息和公务信息等。具有传输主体数量较为有限，范围相对固定的特点。金融机构与外部机构之间，通常采用机构专线或 VPN 进行数据传输。

（2）应用场景数据传输安全风险

- **业务流程图**

- **主要风险点**

  - 传输通道受到破坏
  - 数据传输过程中发生泄露、窃取、篡改等

（3）应用场景数据传输安全解决方案

  - 传输通道受到破坏

管理方面，可建立专用网络和专线安全管理规范，明确专用网络和专线的安全管理要求。

技术方面，可通过部署防火墙等安全设备，应对外部攻击，做好内部网络的漏洞扫描、主动防御等，保证传输通道的安全，并对传输通道进行加密。

- 数据传输过程中发生泄露、窃取、篡改等

管理方面，在建立内部数据传输安全管理机制的同时，金融业机构也应对参与本机构数据传输过程中的第三方机构进行管理，确保不因与第三方机构合作或第三方应用接入而危害数据安全。在向国家机关、行业主管和监管单位传输的数据，严格按照国家及行业相关管理要求进行传输。

技术方面，传输至第三方处理的敏感数据，应事先依据“最小、必要”原则采用数据脱敏技术等进行处理。应对数据传输双方进行不同深度的鉴别、身份认证和账户准入控制，采用安全的密码技术保证数据的完整性、不可抵赖性、防止数据泄露和保证数据安全性。

6.2.4 面向跨境流动的数据传输

（1）应用场景数据传输需求

跨境流动是指金融机构因业务需要与其海外分支机构或总部、其他境外金融机构、第三方数据处理服务商、境外监管机构或行政与司法部门等之间进行数据跨境传输，传输的数据为包括个人金融信息、企业金融信息以及金融机构运营的业务数据等在内的金融数据，具有高敏感性和高价值性。金融机构将存储在境内的相关金融信息，通过跨境传输平台传输至境外，或境外的机构、组织、个人通过访问跨境业务平台，进行业务办理。

（2）应用场景数据传输安全风险

• 业务流程图

• 主要风险点

- 数据出境的目的、范围、方式等的合法性、正当性、必要性
- 传输通道受到破坏
- 数据传输过程中发生泄露、窃取、篡改
- 境外接收方责任义务确认等

（3）应用场景数据传输安全解决方案

金融数据是金融信息的重要载体，由于金融数据的敏感性，其跨境流动涉及公民个人隐私、金融机构自身利益乃至国家金融安全。

- 数据跨境传输的合法性、正当性、必要性

金融机构在中华人民共和国境内运营中收集和产生的个人信息和重要数据按照国家法律规定，应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

- 传输通道受到破坏

管理方面，可建立传输网络管理规范，明确专用传输网络安全管理要求。

技术方面，可采用防火墙、入侵检测等安全技术或设备，确保数据传输网络的安全性，并对传输通道进行加密，保证传输通道的安全。

- 数据传输过程中发生泄露、窃取、篡改等

管理方面，数据传输应严格遵守国家和地方颁布的法律法规和规章以及行业规范。在向境外提供数据前，应进行风险自评估，并针对可能发生的风险制订应急响应预案，及时处置数据安全事件告警，并在重大事件发生时立即启动应急响应。

技术方面，应加强自身信息技术能力建设，提高数据风险识别和管理能力。数据传输前，应根据法律法规和行业标准对业务数据进行脱敏处理及审批授权，数据应采取数据加密、安全传输通道或安全传输协议进行数据传输，并保留本地备份和转移记录。

- 境外接收方责任义务确认

境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全；与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件等（以下统称法律文件）是否充分约定了数据安全保护责任义务等。

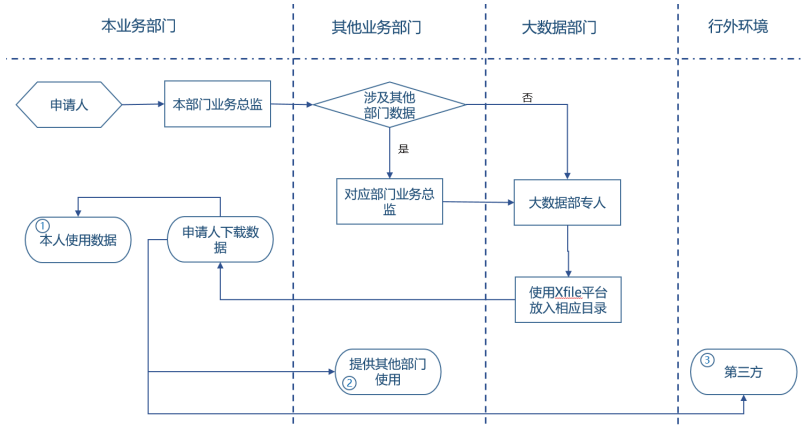
数字金融数据传输安全应用场景 1

需求分析

主体: 发送方是运维团队成员，成员不固定，但范围较小。接收方是数据需求的发起者。全行范围内的所有人员都可以发起需求，需求提出时就标明最终的使用目的和最终使用者。

客体: 各部门都涉及到日常经营数据。数仓中的所有数据，但不涉及4级及以上数据，包含测试场景、数据分析等各种场景。

行为: 通过数据传输平台进行交换。提交下载需求—本部门业务总监审批—（如果涉及其他部门数据，需要相关部门业务总监审批）—大数据部专人审核—提交数据接收人接收目录—接收人通过数据传输平台下载数据。



解决方案

1、管理措施：考虑将下载需求和取数需求的审批流程结合为一体，这样可以直接避免二次审批导致的数据可能存在不一致性的风险。明确系统、数据所属责任部门，并结合到数仓中。明确数据分类分级标准，并在全行范围内发布，以便在审批时，有明确的同意标准。制度中做出明确要求，并提出明确的处罚措施。增加审批人员的删除保证检查。在完成任务后及时删除数据。增加定期、不定期的传输审计行为，对发现违规行为进行通报。对第三方数据安全处理能力做基线要求在第三方的合同中对保密做出明确要求并签署保密协议。

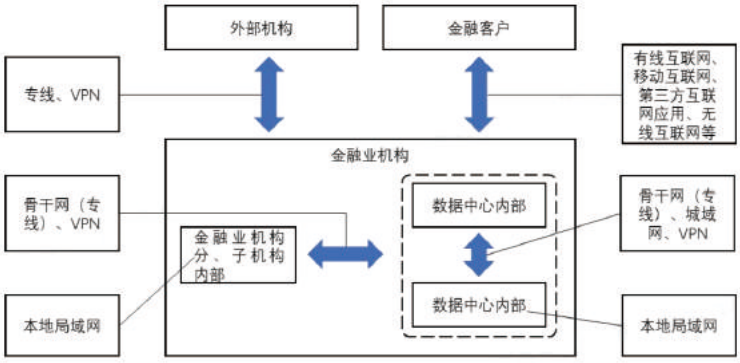
2、技术手段：增加数据安全风险监测设备，包含追踪溯源功能。增加DLP等相关加密及扫描措施。例如邮件DLP。增加文件粉碎等控制措施。采用国密加密算法。

案例 8 数字金融数据传输安全应用场景 2

需求分析

主体：机构内部传输，涉及主体为机构总部、分支及子机构、机构内不同数据中心等。机构外部传输，涉及主体为个人金融信息主体、企业客户、外部数据供应方、外部业务合作机构、政府及监管机构等。数字金融数据传输有数据存在形式多样、数据动态流转复杂、业务数据主体多样、数据价值定义模糊等特点。

客体：聚焦于与外部数据传输，数据按照金融业务维度，主要有风控类数据、零售类数据和对公业务类数据。



解决方案

1、管理措施：按照国家法律和行业技术标准，制定包括传输在内的数据安全管理办法、明确安全责任制、定期开展专项核查、建立专业的运营队伍负责传输安全事件的日常监控和应急处置等。

2、技术手段：加密传输主要通过离线通讯消息加密和在线通讯消息加密。前者包括邮件加密和聊天加密；后者包括基于SSL/TLS的HTTPS,VPN/SDP虚拟网络。此外还需要加强数据传输前主体身份认证，确认通信双方都是可信的。

3、针对外部传输如零售业务场景的开放银行业务，应对内部API接口进行标准统一，对API进行全生命周期管理，通过互联网、专线、移动通信网络等网络通道，部署安全设备，实现网络流量监测和阻断，构建统一API网关，提供权限认证、应用防护及敏感数据识别和加密。

4、针对内部传输中"内部人"有意或无意截取、扩散、更改生产数据为例，在服务端使用集中身份认证平台、数据泄露防护系统、用户行为和数据库审计系统等保障应用传输安全，在客户端部署虚拟桌面、非法外联管控、文档水印等保障客户端传输安全。

案例 9 数字金融数据传输安全应用场景 3

需求分析

主体：数据发送方和接收方均为银行内部人员。

客体：涉及到的数据类型包含程序安装介质、手册文档、系统及应用日志、经营类数据、分析数据等。

行为：传输双方通过跨网文件传输系统进行数据传输，跨网文件传输系统是为解决网络隔离条件下，安全数据传输交换的合规性问题，实现不同网络区域间数据文件的安全传输而建设的信息系统。

解决方案

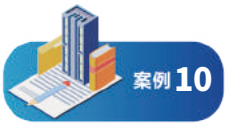
1、系统依照"工作必须、最小范围"的控制原则，对非必须的客户信息须进行脱敏，同时依据"谁申请、谁复核、谁负责"的原则对敏感数据传输进行复核及核查。

2、制定跨网文件传输系统管理细则，明确行内各方职责和工作流程，明确任职干部复核人定义，与行内人力资源系统对接，实现任职和跨网符合工作流程严格匹配，明确权责。

3、建立日常分级检查及监督机制，跨网传输任务清单，每月由跨网文件传输系统管理部门提供基础数据，由总行各部门及分行进行相关信息的核查工作，核查确认相关操作行为是否合规及业务必须。

4、策略核查，每季度针对已经部署实施上线的跨网文件传输系统结合业务场景进行全量策略的评估，不断提升安全策略精准度和覆盖面，增加客户信息保护能力。

5、可对传输的文件在进行应用层DLP之后，对文件进行随机加密，同时将随机密码发送到接收人的邮箱。



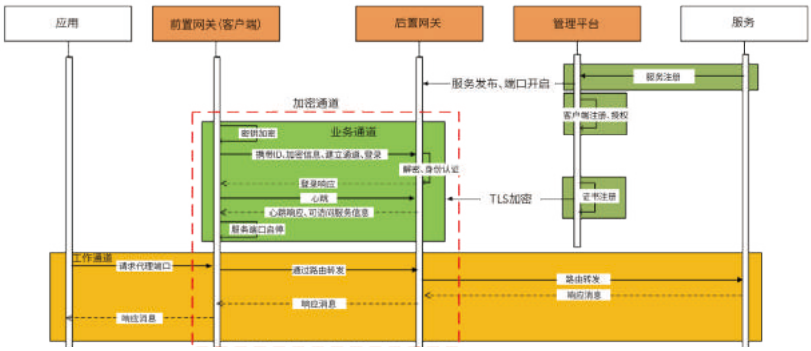
数字金融数据传输安全应用场景 4

需求分析

主体：发送方为金融机构，接收方为相关监管单位。

客体：金融机构与监管单位合作类业务信息。

行为：使用安全接入网关进行数据传输，安全接入网关采用TLS协议保证通讯双方的信息安全，依赖可靠的TCP传输层来传输和接收数据；支持国产加密算法，进行链路数据加密；采取特有应答纠错机制，包括确定应答与重发、记录重组等机制，保证数据包有序、完整到达安全接入网关TLS会话模块。



解决方案

1、系统由前置网关，后置网关，管理控制台三部分构成，其中管理控制台主要负责服务注册，服务的发布，客户端注册，客户端授权，证书管理，日志展示统计等。

2、系统分为信息注册，业务通道，工作通道三部分，信息注册主要包含服务，客户端，证书的注册管理等；业务通道主要负责登录，以及心跳的处理；工作通道负责真正的服务请求；通道均建立在加密通道的基础上。

3、针对HTTP访问应用到前置机存在泄漏风险，采用HTTPS 加密协议访问,可激活客户端浏览器到服务器之间的"SSL加密通道"实现高强度双向加密传输,防止传输数据被泄露或篡改。

4、针对存在非法IP访问风险，通过IP白名单限制访问权限。客户端在注册的时候分配CltID和private_key，客户端登录时对其校验。证书客户端绑定校验证书和CltID进行绑定校验，如果不一致，登录失败。

数字金融数据传输安全应用场景 5

需求分析

主体：传输服务供应商、客户、数据源机构（如涉及）等，均为数据发送方和接收方，其中客户为持牌金融机构，数据源机构为合法合规数据源公司；

客体：传输数据主要包括个人及企业数据；

行为：使通过https进行对外数据传输；

解决方案

1、在组织建设上，建立自上而下的数据安全管理体系，明确相关组织、部门及岗位的数据安全管理职责。

2、在制度建设上，除依照相关法律法规外，参照国家标准化管理委员会、全国金融标准化技术委员会等制定的相关标准，如《信息安全技术个人信息安全规范》《个人金融信息保护技术规范》《金融数据安全 数据安全分级指南》《金融数据安全 数据生命周期安全规范》等，再结合行业最佳实践，制定数据安全管理相关制度，并通过持续运营管理，不断加强安全制度的落地实施。

3、在能力建设上，除不断加强安全管理人员专业水平外，还不断提升全员安全意识等；数据安全是一项需要借助技术解决方案的管理工作。

4、在数据外部传输上，采用签名验签、数据加密、通道加密等技术，确保数据的保密性、完整性及可用性。如在与B机构进行数据传输的过程中，通过https传输传送数据给B机构，其中主要应用数字证书、数字签名、身份验证、参数验签、ACL 访问控制列表、防重放、数字信封等技术。

案例 12 数字金融数据传输安全应用场景 6

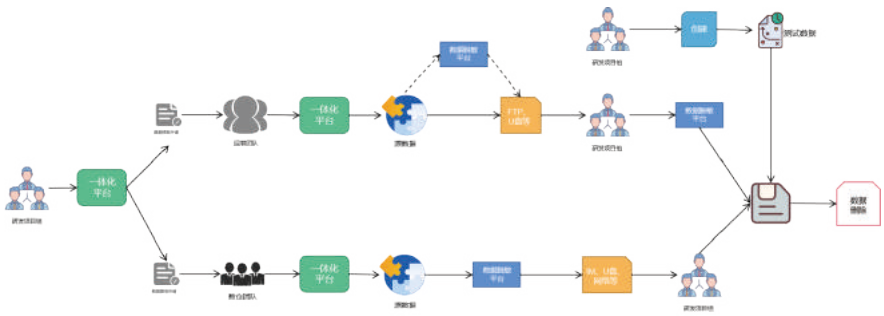
需求分析

1、研发测试数据使用场景

主体：金融机构系统和应用的研发工作一般由软件开发部门负责，以合作开发的模式为主按照系统来成立研发项目组，金融机构人员负责管理和技术方案的制定，外包人员负责主体研发工作。

客体：“监管报送信息”类别下的监管上报信息；“业务数据”类别下的各类业务数据。

行为：研发测试数据提取申请单通过审批后，可以通过运维团队、数据管理团队或数据管理平台团队将数据从备份系统、数据仓库、数据服务平台中下载到办公终端。数据处理环境包括安全U盘、FTP服务器、IM软件、一体化平台。



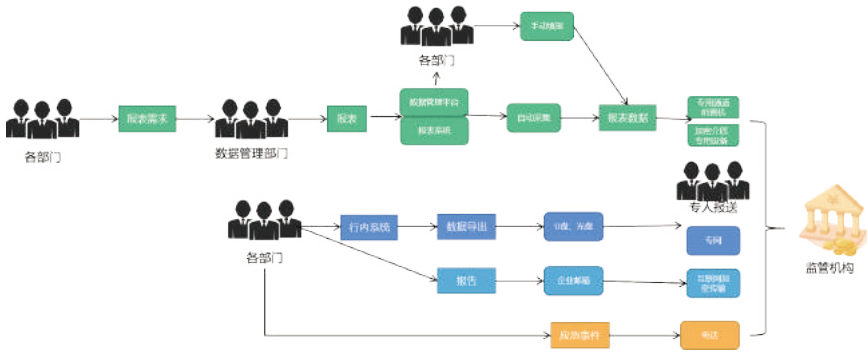
2、监管数据报送场景

主体：为了防范风险，保证金融市场的稳定，人行和银保监会需要了解汇总银行情况，各银行需要按要求进行数据报送。金融机构各分级行、总行部室、直属机构均需要按照监管要求报送数据。

客体：“监管报送信息”，总体构成以3级数据为主，存在部分2级数据，例如资产负债数据、信贷数据、银行账簿利率风险计量数据等。

行为：线上报送采用数据管理平台中将监管报表通过专线、前置机传输到监管单位的对应服

务器上；线下报送方式由专人从系统上下载报表后，保存到安全U盘中，通过专人报送至监管机构；报告类数据加密后通过外网的企业邮箱传输给监管机构；通过电话报送等多种数据传输形式，报送数据的传输方式通常由监管机构指定。数据处理环境为数据服务平台、U盘、光盘、企业电子邮箱系统等。



解决方案

1、针对开发测试场景中的风险点，数据管理部门应建立数据分类分级制度，并明确各级数据在各阶段的安全管控要求；通过数据分类分级工具对数据资产进行识别、管理并制定防护措施；建立健全数据提取的申请、审批及定期跟踪流程；内网数据导出要使用专用内部安全U盘，并建立安全U盘使用管理流程；采用静态脱敏的技术手段针对研发测试场景下的测试的真实数据提前进行脱敏，避免真实数据泄漏；采用重识别等技术手段对脱敏后的数据进行风险评估，校验脱敏策略的有效性；采用数据库审计的技术手段针对数据提取过程中的人员行为进行记录，定期进行复核审计避免数据泄露。

2、针对监管数据报送场景中的风险点，数据管理部门应建立数据分类分级制度，并明确各级数据在各阶段的安全管控要求；通过数据分类分级工具对数据资产进行识别、控制，并制定防护措施；通过互联网邮箱向监管部门报送的信息需要加密；外网出口设上网行为管控，记录员工的上网行为，上网行为等日志由异地灾备和技术保障处定期上交总行风险部门；内网各网络间和外网出口部署数据防泄漏设备，监测敏感数据的流动，发现异常行为进行告警，同时，提升员工敏感数据防范意识，降低内部员工无意泄漏敏感数据的风险。

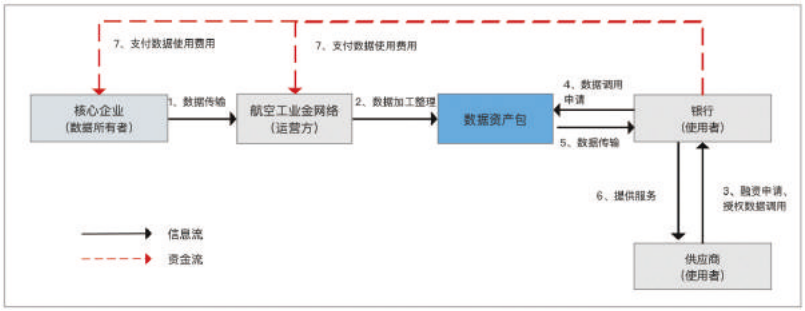
案例 13 数字金融数据传输安全应用场景 7

需求分析

主体：数据的所有者、运营者和使用者。航空供应链核心企业是数据要素的所有者、控制者和管理者。数据运营者通过利用物联网、区块链、隐私计算、电子签名等技术提供数据调用、数据上链等技术和运营服务。数据的使用者为需要集中获客、购买数据、使用数据作为授信依据的金融机构以及有融资需求的供应商。

客体：由核心企业确认的供应商上下游生产协同数据，包括采购计划、电子合同、生产进度、质量检验、仓储物流、发票结算、往来对账、资金计划等。

行为：数据运营者负责数据传输相关技术的基础设施建设以及数据安全管理运营方。数据使用者在获取授权及支付使用费用之后，可以通过数据运营者获取所有者管理的数据。



解决方案

1、传输的数据要素内容、格式等是否符合使用者需求，数据传输前，确认数据使用者所需要的数据要素内容及格式并在协议中进行相关约定，传输双方出具标准化接口文档。

2、数据传输过程的数据泄露：从管理方面，可对内外传输通道和访问终端账户进行管控，确保数据传输过程中不会被泄露、篡改、伪造及窃取等。从技术方面，采用安全的自主研发技术平台，在对外和对内的数据传输过程中，采取相应的安全网络隔离，入侵检测访问控制设备和内部服务端防火墙安全部署，对外金融机构终端进行鉴别和客户账户准入控制，通信访问平台进行不同深度的身份认证，采用安全的密码技术保证数据的完整性、不可抵赖性、防止数据泄露和保证数据安全性。通信中采用专线或VPN等技术确保传输通道安全，并对数据进行加密，高等级关键数据原则上不对外传输，确实业务需要则需要审批并保证数据保密性。

3、物理介质传输：需要对数据进行技术加密或脱敏，并有专人负责，并保证传输介质物理安全，不在无人监管情况下通过第三方传递。

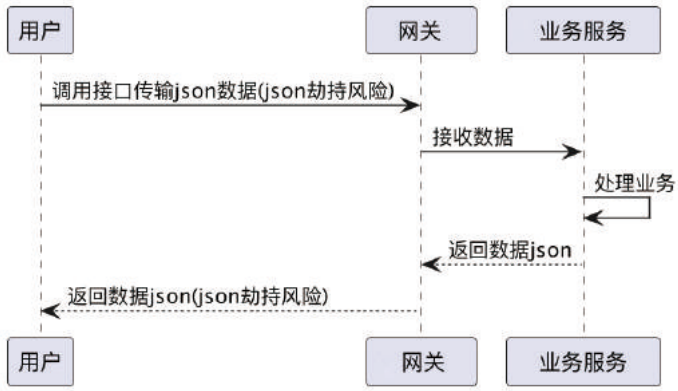
数字金融数据传输安全应用场景 8

需求分析

主体：发送方平台客户，接收方为税务申报平台。

客体：税务申报业务数据，格式为JSON。

行为：通过开放API同步税务申报的业务数据到SaaS税务申报平台。



解决方案

1、针对Json劫持漏洞风险，一是可以限制referer来源，利用前端referer的不可伪造性来保障请求数据的应用来源于可信的端或者应用，但在某些情况下（如存在xss跨站脚本攻击）攻击者可能绕过该防护措施。二是可加入token验证，利用token身份认证临时令牌，对调用者的身份进行认证，这种方式对于调用者的身份要求力度较细，但是一旦出现xss也可能导致前端token的泄露，从而导致保护失效。

2、针对水平越权、垂直越权、参数遍历风险，一是可支持外部openID，此ID使用雪花算法生成，无规律，无法被遍历；二是使用ID加密，自增的ID通过加密算法，无法被遍历。

七、互联网应用场景

互联网已经融入经济社会生产和生活各个领域，用户规模及普及率不断提高，基础网络和数据资源日趋丰富，新模式新业态层出不穷带来新风险。

7.1 互联网总体情况

互联网已经融入经济社会生产和生活各个领域,带来新的生活方式和商业模式，教育、医疗、养老、抚幼、就业、文体、助残等重点领域数字化普惠应用发展迅速，互联网的普及带动了数字社会总体建设步伐加快。

互联网用户规模及普及率不断提高。根据中国互联网络信息中心发布的《中国互联网络发展状况统计报告》显示，2011-2021年我国互联网网民数量及互联网普及率稳定上升，我国互联网普及率已超七成。截至2021年底，我国网民规模达突破10.32亿,形成全球最大网民群体。我国互联网行为特点为每周人均上网时间保持增长，上网终端设备使用场景更加多元。

互联网基础网络和数据资源日趋丰富。《数字中国发展报告（2021年）》指出，2017年到2021年，我国数据产量从2.3ZB增长至6.6ZB。截至2021年底，我国已建成142.5万个5G基站，总量占全球60%以上，5G用户数达到3.55亿户，IPv6地址资源总量位居世界第一，IPv6活跃用户数达6.08亿。目前，我国工业互联网应用已覆盖45个国民经济大类，电子商务交易额从2017年的29万亿元增长至2021年的42万亿元。

互联网行业领域数据安全规范逐步完善。近年来，《网络安全法》《数据安全法》《个人信息保护法》的先后出台实施，以及国家互联网信息办公室发布了《网络数据安全管理条例（征求意见稿）》《数据出境安全评估办法》等一系列数据安全法律法规制度文件，为互联网行业领域的创新发展和健康发展夯实了基础。

云网融合背景下新模式新业态层出不穷带来新风险。由于敏捷性需求和微服务架构的发展，越来越多互联网应用开始通过云部署，提供云服务。API已成为数字时代网络应用流量最重要的出入口，通过攻击API来破坏信息系统和窃取数据成为新风险点，亟需加强安全资源整合，加强API运行时安全状态防护，构建安全的数字生态系统。

7.2 互联网数据传输场景及解决方案

互联网数据传输安全应用场景主要分为面向用户和用户之间信息分享的数据传输、面向平台向用户提供服务的数据传输、面向平台和平台之间信息共享的数据传输、面向跨境流动的数据传输，各应用场景的主体、客体、行为和特点如表所示。

序号	应用场景	主体	客体	行为	特点
1	面向用户和用户之间信息分享的数据传输	分享信息的用户	用户之间分享的信息	数据从发送信息的客户端通过服务器传输到接收信息的客户端	发送方请求量大且分布广泛，数据涉及个人隐私
2	面向平台向用户提供服务的数据传输	用户、提供服务的平台	用户信息、业务数据等	数据从用户客户端发传输到服务器	发送方具有分布广泛且请求数量大的特点
3	面向平台和平台之间信息共享的数据传输	分享数据的平台	业务数据等	数据从发送数据的服务器传输到接收数据的服务器	发送方和接收方传输接口安全建设标准不统一
4	面向跨境流动的数据传输	境内互联网企业、境外其分支机构或第三方机构	需要跨境传输的相关数据	境内数据处理者将数据传输、存储至境外；数据处理者境内存储的数据让境外的机构、组织或者个人访问	合规评估复杂，境外屡责落实难

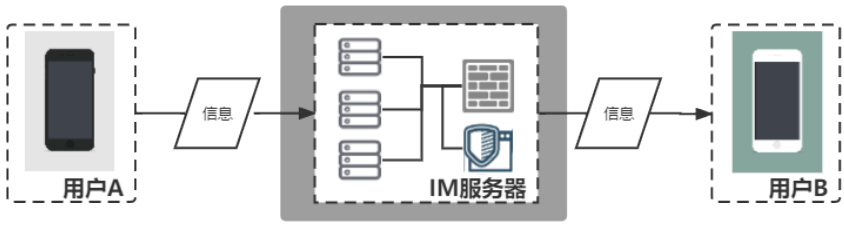
7.2.1 面向用户与用户之间信息分享的数据传输

（1）应用场景数据传输需求

用户与用户之间的信息共享的数据传输路径为用户客户端与到用户客户端之间数据传输。传输的发送方为客户端A，接收方为客户端B，具有发送与接收延时小快速传输的特点。通过A要给用户B发送一条消息，这个消息会先发送到IM服务器，再由IM服务器发送给B。

（2）应用场景数据传输安全风险

- **业务流程图**



- **主要风险点**

  - 消息数据在发送途中被劫持或篡改
  - 消息数据发送不完整

（3）应用场景数据传输安全解决方案

  - 消息数据的在发送途中被劫持或篡改

管理方面，利用信息保护较高、相对成熟的app，明确app产品和服务过程中信息安全管理责任与保密责任。

技术方面，利用数据加密技术、安全传输技术。在利用可靠数据传输协议

的情况下，用户A在发送之前把消息加密处理封装成数据包发给IM服务器，IM服务器把数据包发送给接收消息的用户。

- 消息数据发送不完整

管理方面，制定信息确认机制、错误报送机制、内容信息校验机制，保证在安全互联网环境中进行数据传输。

技术方面，利用可靠传输协议传输客户端发送信息，利用逻辑校验的方式与编程校验的方式进行确认，保证消息送达。

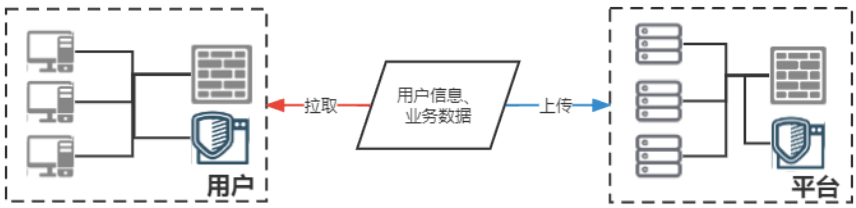
7.2.2 面向平台向用户提供服务的数据传输

（1）应用场景数据传输需求

平台向用户提供服务的数据传输路径为用户通过客户端将数据传输到平台，发送方具有分布广泛且请求数量大的特点。传输的数据一般为业务数据以及必要的用户信息，按照传输方式可分为客户端从后端接口拉取数据和客户端向后端接口上传数据这两种方式。当用户在客户端发起请求向平台后端接口上传或者拉取数据时，后端服务器会进行身份确认后，将接收到的处理结果反馈。

（2）应用场景数据传输安全风险

- **业务流程图**



• 主要风险点

- 客户端伪造风险
- 身份鉴别信息泄漏风险
- 数据泄漏及遭受攻击风险

（3）应用场景数据传输安全解决方案

- 客户端伪造风险

管理方面，应建立平台信息保护组织架构，明确在提供平台产品和服务的过程中数据安全管理规范，明确数据传输管理要求。并针对相关岗位明确其互联网信息安全管理责任。

技术方面，客户端被篡改或者伪造，造成中间人窃取关键数据或者爬虫批量获取后端数据等风险。可以通过使用客户端加壳、完整性校验、密钥双向校验等技术措施，降低客户端伪造风险。

- 身份鉴别信息泄漏风险

管理方面，通过制定身份鉴别信息保存、鉴别和加密机制，规范业务交互过程中的身份鉴别处理机制等管理措施。

技术方面，对加密的加密方法、密钥强度等做出升级，降低关键数据被泄漏及解密的风险。

- 数据泄漏及遭受攻击风险

数据库由于权限管理不到位或者权限策略不细致，造成数据泄漏或越权访问。

管理方面，通过统一的数据中台，集中对数据库权限的申请、管理、修改等进行管理方式，明确权限责任人，周期性权限轮换制度。

技术方面，提供统一的数据读取的接口和申请机制，保证数据库权限的收敛和最小化原则。

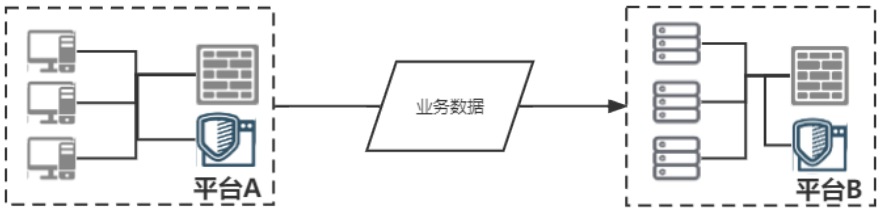
7.2.3 面向平台和平台之间信息共享的数据传输

（1）应用场景数据传输需求

面向平台和平台之间信息共享的数据传输路径为第三方平台利用客户端调用平台后端的数据，传输的一般为业务数据，按照传输方式可分为客户端从后端接口拉取数据和客户端向后端接口上传数据这两种方式。第三方平台与服务端之间的数据传输除使用HTTPS的方式进行数据交换外，会额外增加多项安全措施，会针对第三方平台的IP进行访问控制，引入证书签名机制，对数据信息报文进行签名验签等，保障数据真实有效。

（2）应用场景数据传输安全风险

- **业务流程图**



- **主要风险点**

  - 客户端伪造风险
  - 身份鉴别信息泄漏风险

- 数据泄漏及遭受攻击风险

（3）应用场景数据传输安全解决方案

- 客户端伪造风险

管理方面，应建立平台信息保护组织架构，明确在提供平台产品和服务的过程中数据安全管理规范，明确数据传输管理要求。并针对相关岗位明确其互联网信息安全管理责任。

技术方面，可以通过使用客户端加壳、完整性校验、密钥双向校验等技术措施，降低客户端伪造风险。

- 身份鉴别信息泄漏风险

管理方面，通过制定身份鉴别信息保存、鉴别和加密机制，规范业务交互过程中的身份鉴别处理机制，明确岗位责任人等管理手段。

技术方面，对加密的加密方法、密钥强度等做出升级，降低关键数据被泄漏及解密的风险。引入证书签名机制，对数据信息报文进行签名验签，针对开放接口，保障数据真实有效。

- 数据泄漏及遭受攻击风险

数据库由于应用程序漏洞或者中间件组件漏洞，造成数据库管理数据及关键业务数据泄漏、篡改、删除等风险。

管理方面，定期对应用程序和中间件组件进行安全测试，发现潜在的安全隐患并及时修复，准确识别可疑风险，竭力将风险降到最低。

技术方面，建立数据安全管理平台，对业务流程中数据流转进行有效监控。

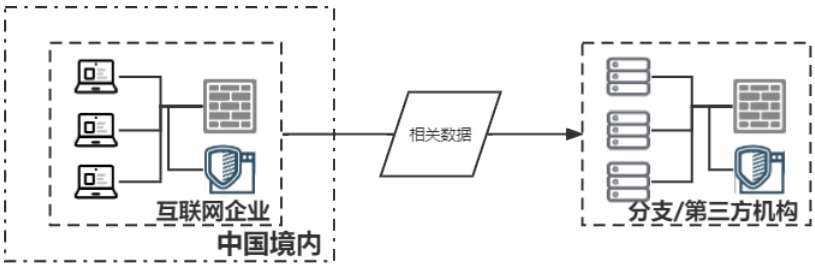
7.2.4 面向跨境流动的数据传输

（1）应用场景数据传输需求

跨境流动传输是指互联网企业因业务需要与其海外分支机构或总部、其他境外机构、第三方数据处理服务商、境外监管机构或行政与司法部门等之间进行数据跨境传输，传输的数据为包括需要跨境的个人信息、企业信息以及互联网机构运营的业务数据等之内的相关业务数据，具有高敏感性和高价值性。一是数据处理者将在境内运营中收集和产生的数据传输、存储至境外。二是数据处理者收集和产生的数据存储在境内，境外的机构、组织或者个人可以访问或者调用。

（2）应用场景数据传输安全风险

- **业务流程图**



- **主要风险点**

  - 数据出境的目的、范围、方式等的合法性、正当性、必要性。

  - 出境数据的规模、范围、种类、敏感程度，出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险。

  - 数据安全和个人信息权益是否能够得到充分有效保障。

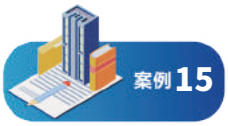
  - 数据处理者与境外接收方拟订立的法律文件中是否充分约定了数据安全保

护责任义务，以及遵守中国法律、行政法规、部门规章等情况。

（3）应用场景数据传输安全解决方案

管理方面，依据《数据出境安全评估办法》等相关法律法规制定数据出境风险自评估流程。符合数据出境安全制度的，向相关部门申报评估出入境数据，申报材料通过后，才可以进行相关数据出境动作，反之进行整改再次申报。

技术方面， 利用数据本地化存储、数据加密存储技术、 数据安全使用技术、数据安全传输技术、匿名化和去标识化处理技术、个人信息保护认证保证跨境传输数据安全。



互联网数据传输安全应用场景 1

需求分析

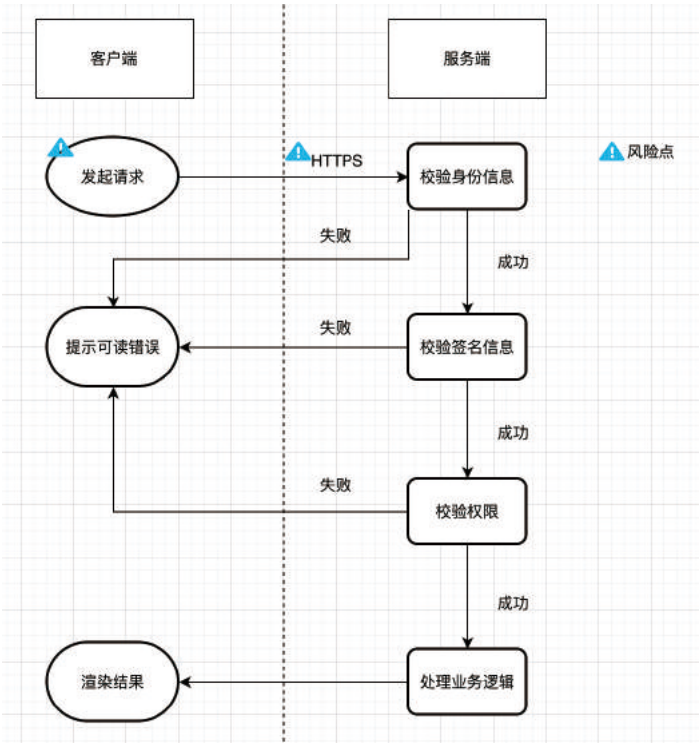
主体: 发送方一般由两部分组成，一部分为移动端和网页Web端用户。终端节点环境复杂，业务形态类型多种多样，数据庞大繁杂，不同数据的采集传输方式各不相同。另一部分第三方合作伙伴。第三方服务安全建设参差不齐，各服务之间无统一模版标准，定制化程度高。接收方为后端服务器。与客户端进行各类数据交换服务，具备统一的API网关，使信息收敛。

客体: 业务数据或必要的用户信息。

行为:

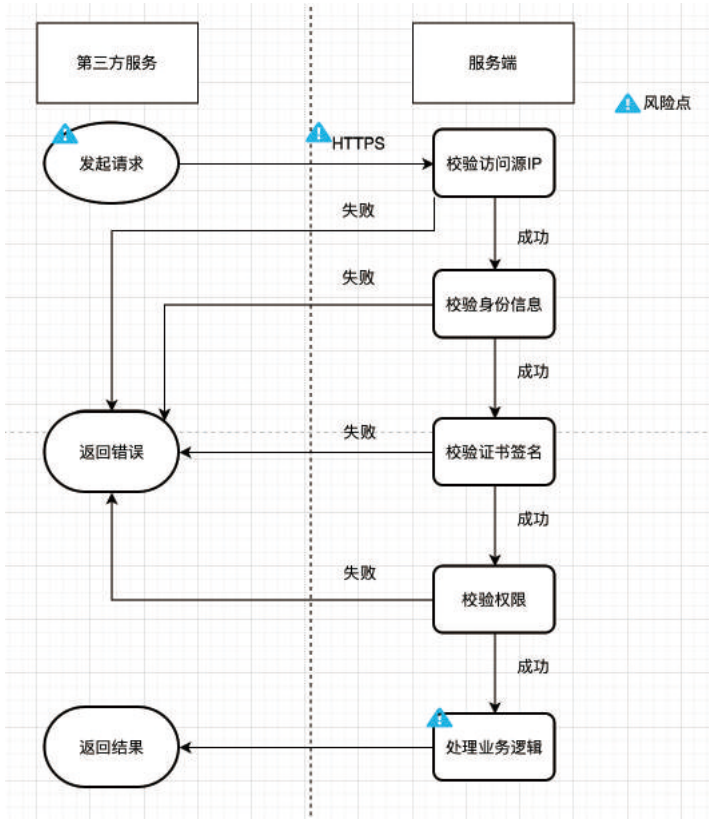
1、客户端与服务端之间的数据传输：

客户端与服务端传输主要保证数据传输过程中的保密性、完整性、不可抵赖性，通过HTTPS传输协议进行数据交换，针对敏感操作接口在报文中额外增加签名验签的校验机制，签名密钥基于用户身份计算得出，保证用户唯一密钥唯一。



2、第三方服务与服务端之间的数据传输：

第三方服务与服务端之间的数据传输除使用HTTPS的方式进行数据交换外，会额外增加多项安全措施，会针对第三方服务的IP进行访问控制，引入证书签名机制，对数据信息报文进行签名验签，保障数据真实有效。

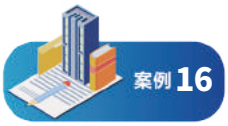


解决方案

1、针对客户端伪造风险、第三方服务风险遭受攻击数据泄露风险、第三方服务风险，通过制定健全的安全编码设计文档，定期向研发人员对数据传输过程中的安全要求和规定进行宣贯；制定严谨的第三方服务合作安全协议，明确安全风险的责任制；制定应急演练流程，定期进行数据安全应急演练，尽力做到防范于未然。

2、针对客户端伪造风险，组建技术安全团队对客户端进行安全加固，包括不限于代码混淆、抗调试等对抗方法，增加攻击成本，降低客户端遭受的风险。

3、针对第三方服务风险和数据泄露风险，通过定期授权的安全测试，对服务接口进行安全测试，发现潜在的安全隐患并及时修复，同时研发数据安全管理平台，对业务流程中数据流转进行有效监控，准确识别可疑风险，竭力将风险降到最低。



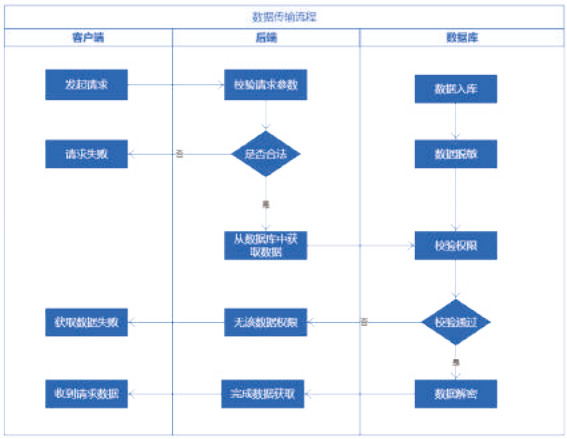
互联网数据传输安全应用场景 2

需求分析

主体: 发送方为主站客户端程序，客户端分布广泛且请求数量大，部署在客户移动终端。接收方为后端应用程序接口，接口数量同样众多，但主要部署在集团IDC及各云平台上，管理方式相对集中。

客体: 客户信息、订单数据、业务数据等。

行为: 户客户端和后端接口有多种数据传输的场景，按照传输方式可分为客户端从后端接口拉取数据和客户端向后端接口上传数据这两种方式。当客户端发起请求向后端接口上传或者拉取数据时，后端服务器会校验身份信息，成功后反馈处理结果。



解决方案

1、通过对目前业务中数据传输场景，从客户端到服务后端的改造和治理措施，降低了数据传输链路和各环节中的风险；通过数据中台对数据权限和接口的统一管理和收敛，从业务方面完善了数据传输的风险收敛。

2、通过制定身份鉴别信息保存、鉴别和加密机制，规范业务交互过程中的身份鉴别处理机制、统一的数据中台，集中对数据库权限的申请、管理、修改，提供统一的数据读取的接口和申请机制，保证数据库权限的收敛和最小化原则。

3、通过使用客户端加壳、完整性校验、密钥双向校验，对加密的加密方法、密钥强度进行升级。通过对目前业务中数据传输场景，从客户端到服务后端的改造和治理措施，降低了数据传输链路和各环节中的风险。并且，通过数据中台对数据权限和接口的统一管理和收敛，从业务方面完善了数据传输的风险收敛。

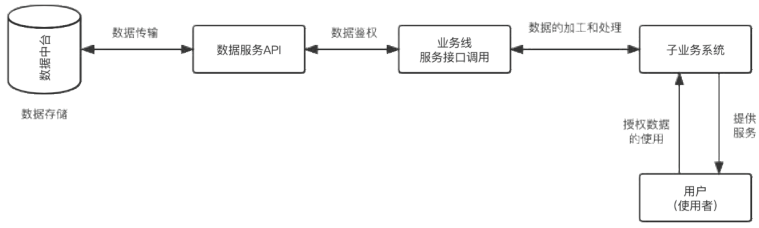
互联网数据传输安全应用场景 3

需求分析

主体: 发送方为企业内部各个业务线的分支机构和部门，业务方众多，使用的接口数量也比较庞大。接收方为企业内部的数据中台，接收的数据体量大，数据类型不固定。

客体: 订单信息、用户信息以及其它业务数据。

行为: 各个业务线和数据中台的数据传输方式有多种场景，按照数据传输的方式可分为数据的查询与数据的上报。以上两种场景都是通过API接口来进行数据的传输，数据中台会在接口被调用时进行鉴权，鉴权通过后方可正常进行数据传输，否则返回异常信息。



解决方案

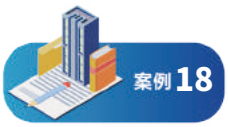
1、通过建设API网关，对数据的权限、访问、日志等进行管控，使用数据签名的机制确保数据在传输过程中不会被泄漏、伪造、篡改。

2、通过建设鉴权信息集中化管理和存储平台、建成硬编码扫描能力、设立代码开源审批流程等方式降低数据接口鉴权信息泄漏风险。

3、通过建设安全巡检能力，定期对提供数据服务所涉及的组件、平台进行安全测试，发现存在的安全问题使用工单流程追踪和修复。

4、通过建成威胁情报平台，第一时间感知数据服务相关组件的漏洞讯息，及时跟进和升级。

5、通过和业务共建的方式，建成一套API管控平台，梳理和标记业务数据中存在的敏感数据类型和等级，推进数据安全治理，对于数据的使用采取最小化原则，敏感数据采用脱敏的方式参与业务。



互联网数据传输安全应用场景 4

需求分析

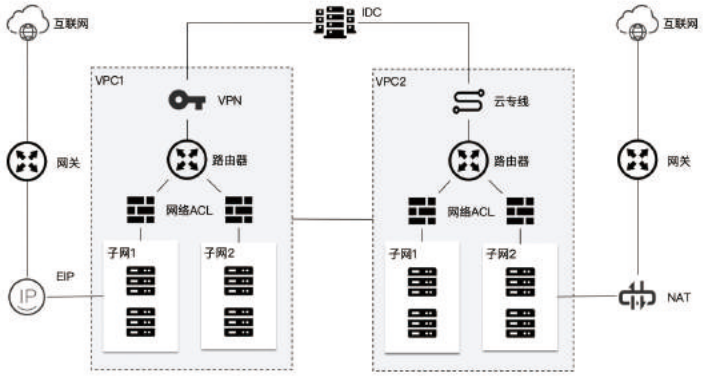
主体: 互联网用户、企业、云平台。互联网用户侧传输主要指对公众开放的业务使用时产生的数据传输，企业侧主要指企业内部间的数据传输，云平台侧即为云内传输，以及跨云、多云之间的数据传输，也包括云-边之间的互联互通。

客体: 主要建立管控的数据分为企业数据、用户数据、IT数据。

行为: 一是云内通信，云内的虚拟化子网以VPC结构进行切分，其中每个VPC内部通过VPN进行信道控制，同时具有负载均衡和ACL控制，同时在每个VPC内部建立子网，子网之间可以通过安全组定义互通链路，此部分允许云租户在默认网络架构基础上自定义符合业务的通信模式。

二是云地通信，企业IDC机房通常可以通过VPC或专线的方式接入云平台，IDC内部根据企业网络规划，多由互联网出口交换，到核心交换，到各个网络分析内部的核心交换与准入交换节点。

三是云网通信，租户在云端租用的资源可以通过虚拟IP池的方式直通互联网，同时可以通过NAT进行映射配置，在铜线链路中也包含负载均衡、网络准入、防火墙及其他串行流控措施。



解决方案

1、通过数据安全具体管理制度体系的建设和执行，包括数据安全方针和总体建设思路、数据安全管理规范、数据安全操作指南、数据安全应急作业指导，提供流程并通过相关的在线系统进行支撑。

2、通过保证与制度流程相配套的有效执行的技术和工具，通过内部安全运营平台、数据安全管控工具等部分组成，横跨IT、业务、安全三个职责，并制作与其职能相对应的流程平台，同时将部分技术工具开放提供给企业及云平台用户。

3、通过针对数据安全管理能力、数据安全运营能力、数据安全技术能力及数据安全合规能力培养复合型人才，根据不同数据安全能力建设需要匹配不同人员能力要求。

八、趋势展望

充分发挥数据规模和数据应用优势，更好释放数据红利，加强数据安全监管，营造安全有序的市场环境。

•战略高度和重要价值

提升对数据传输安全重要意义的认识，聚焦数据传输环节，规范数据处理活动，保障数据安全，促进数据资源的高效开发利用和安全有序流动。

•顶层设计和体系建设

推动业务与安全体系深入融合，基于业务特点，跨部门统筹做好数据分类分级，建立层次清晰、职责明确的安全合规体系，全面落实个人信息保护与数据安全等责任义务。

•技术应用和需求牵引

保障关键信息基础设施相关产业链供应链安全稳定，加强数据传输安全需求方建设经验实践的分享交流，打造分领域分行业案例库策略库。

•监管审计和培训考核

关注数据跨境传输等监管新规，深入研究并探索制定可执行可落地的行业监管审计标准指南，鼓励相关行业企业加强合规培训，增强数据传输安全保护责任意识。

后记

《数据安全法》已于2021年9月1日正式落地施行，数据安全产业进入了高速发展期，已经成为保障数字经济健康发展的基石。面对数据传输安全层出不穷的应用场景，机遇和挑战并存。

本次《数据传输安全白皮书》编制，由工业和信息化部网络安全产业发展中心（工业和信息化部信息中心）牵头组织编制，主要聚焦数字政府建设、数字金融、互联网等领域中数据传输安全应用较为典型的场景。后续我们将集聚更多数据安全产业的优势资源，深耕数据存储安全、数据使用安全、数据加工安全等领域，诚邀产业各界协同合作，共绘数据安全产业发展新图景！

在此，编制组向在编制过程中，得到的政府部门、地方园区、行业用户的大力支持，表示衷心感谢！向所有给予指导和帮助的领导、专家、企业和机构，表示衷心感谢！书中难免存在一定疏漏和不足，敬请广大读者提出宝贵意见和建议。

地址:
北京海淀区万寿路27号院

邮编:
100846

官网:
http://www.miitxxzx.org.cn/