数据安全治理白皮书

杭州安恒信息技术股份有限公司

上海赛博网络安全产业创新研究院

2019 年 4 月

目录

1 全球数据安全治理现状

随着国家大数据战略的不断推动深化，大数据驱动的产业创新层出不穷，各种“互联网+”应用和服务大大缩短了企业和用户的距离。人工智能等技术在城市治理、金融、医疗、交通、家居、制造等领域广泛应用，数据采集终端越来越多，传输速度越来越快。个人用户成为万物互联、人机交互、天地一体的智能化网络空间中的重要数据生产者和消费者。作为机器学习、深度学习等人工智能技术的根基，数据也成为了“智能+”时代企业制胜的法宝。与此同时，数据作为重要资产，受到安全威胁的程度也越来越严重，数据遭滥用和泄露的现象极为普遍，个人隐私保护面临重大挑战。

1.1 全球数据泄露事件高居不下

安全情报提供商 Risk Based Security(RBS)发布的一份报告显示，2018 年全球公开披露的数据泄露事件超过 6500 起，共泄露信息超过 50 亿条。其中，有三分之二来自企业，来自政府、医疗和教育部门的数据泄露事件分别占 13.9%、13.4%和 6.5%。值得注意的是，这其中有 12 起数据泄露事件涉及超 1 亿条信息。

2018 年以来，从涉及人数、舆论关注程度、经济赔偿额度三个方面具有代表性的大规模数据泄露事件包括：

- 印度公民身份数据库 Aadhaar 数据泄露

2018 年 1 月，印度 11 亿公民身份数据库 Aadhaar 被曝遭网络攻击，该数据库除了姓名、电话号码、邮箱地址、照片等数据之外，还

包括指纹、虹膜纪录等极度敏感的个人信息。

- Facebook 数据泄露

2018 年 3 月，媒体揭露称一家服务特朗普竞选团队的数据分析公司 Cambridge Analytica 获得了 Facebook 数千万用户的数据，并进行违规滥用。随后 Facebook 宣布有 8700 万用户受到影响。2019 年 4 月初，Facebook 再度被曝 5.4 亿条用户数据在亚马逊云服务器上遭第三方公司泄露。

- 雅虎因数据泄露事件赔偿 1.175 亿美元

2019 年 4 月 10 日，由于遭遇史上最大数据泄密事件，雅虎接受了一项修改后的 1.175 亿美元和解协议，与本案的数百万受害者达成和解。这起案件在 2013 至 2016 年间导致大约 30 亿帐号受到影响，而雅虎则被控在披露此事的过程中反应过慢。

1.2 用户数据保护意识大大提升

随着数据泄露、数据滥用事件不断爆发，用户对个人信息保护的意识正不断增强。据调查报告显示，来自美国和欧洲的 7500 多名受访者中有 73%的人表示，与五年前相比，他们对数据泄露的意识有所增强。其中，当涉及到个人信息丢失时，消费者最关心的是财务、安全和身份数据。其次，接近 50%的用户承认在网上注册产品和服务时，会出于安全或避免营销等考虑故意伪造个人信息和数据。同时，大部分用户正减少他们在网上或与公司分享的个人信息的数量，用户也大多不会将数据交给未经用户同意而销售或滥用数据的公司。

此外，随着用户数据被更加广泛的使用和分析，消费者对个性化

服务的态度也正快速发生转化，由之前的接受变为越来越排斥。同时，认为“拥有更多客户数据的公司能够提供更好、更个性化的产品和服务”的用户也越来越少。

由此可见，高居不下的数据泄露及不道德的数据使用事件正使得消费者对数据共享越来越持保守态度，同时数据和隐私保护能力正逐渐成为消费者权衡是否购买企业产品和服务的重要因素之一。

1.3 各国数据安全监管艰难前行

当前，随着大数据、人工智能等技术的快速发展，面对严峻的数据安全和隐私保护形势，全球各国监管机构都积极应对，力图通过立法加强企业/组织的数据保护主体责任。截至目前，全球有超过 100 个国家和地区制定了专门的个人信息保护法，包括欧盟、俄罗斯、美国加州、印度等地。然而，数据安全法规的实施和执行并不顺畅，尤其是对于已掌握海量数据的科技公司来说，难以即时完成数据梳理并落实满足法律法规要求的数据保护措施。

在欧洲，2018 年 5 月 GDPR 正式实施后，社会隐私组织和监管机构都将目光投向谷歌、Facebook、亚马逊等全球科技巨头，开展数据隐私保护审查。其中，谷歌已因违反 GDPR 而被法国数据保护监管机构处以 5000 万欧元罚款。同时，这些科技公司也遭到了来自俄罗斯、日本等地监管机构的调查和起诉，例如 2019 年 1 月俄罗斯通信监管机构宣布对 Facebook 和 Twitter 发起民事诉讼，原因是这两家公司未能履行俄罗斯的数据保护法。

从全球来看，各国数据安全监管才刚刚起航，科技巨头首当其冲，

成为被监管的首要对象和关注焦点。然而，数据安全监管的道路任重而道远，如何平衡数据安全保障和数据价值实现仍是亟待解决的全球难题。同时，有效实施监管需要建立多层次的监管体系。

1.4 数据安全建设助力企业发展

在风险、业务及合规驱动下，全球数据安全需求全面激活。数据安全厂商也顺应数字技术发展趋势，变革数据安全技术，为企业建设数据安全能力提供可靠有效的解决方案。当前，企业的数据安全需求包括：

- **合规性需求。**从全球范围来看，无论国内还是国外，随着用户的数据保护意识不断增强，以及制定数据保护法规的热潮在全球继续蔓延，企业将面临越来越大的合规性挑战。
- **隐私保护。**在数据安全范畴内，隐私保护将日益成为企业开展业务需直面的难题。隐私数据发现、数据流动追溯、数据脱敏、差分隐私保护、隐私数据泄露监控等技术将成为必需。
- **细粒度的数据分类分级。**随着越来越多的企业成为“大数据公司”，更加细粒度的数据分类分级技术是企业保护海量数据的前提。
- **现代化的数据安全工具。**随着企业的数字化转型和 IT 环境的改变，企业更加需要能够简化数据安全场景和降低复杂性的解决方案，同时，这些工具应能够既涵盖企业内部传统安全问题，又能适应现代的、基于云的数字转型技术。

2 数据安全面临的挑战

2.1 业务视角下，数据价值凸显，管控能力不足

（一） 缺乏对海量用户、数据的安全管理能力

过去几年间，网络和系统中的数据量、用户量一直保持迅猛增长。某专业机构研究报告显示，2018 年中国产生了大约 7.6ZB 的数据，全球互联网在 2018 年平均每天增加超过一百万的新用户。智能家居、智能汽车、可穿戴设备、智能医疗等智能设备的广泛应用也即将带来数据量的又一次飞跃。

数据和用户的大量汇集加大了访问授权的难度，产生了新的业务风险。系统管理员无法及时对海量用户进行权限配置和更新，使得过度授权和授权不足的现象同时存在。各种半结构化、非结构化的数据难以通过访问策略精确描述和控制访问范围，同样导致粗粒度访问控制问题。

（二） 缺乏数据生命周期监控能力

在分布式的部署架构、开放的网络环境中，频繁的数据共享和交换使得数据流动路径变得交错复杂，系统、业务、组织的边界模糊，数据安全责任难以界定。安全策略、管理制度和操作规程等未能落实到数据整个生命周期的各个管控环节，也缺少有效的数据自动化分类分级措施、敏感数据的存储加密和共享脱敏手段、数据交换共享的合规性监控、数据生命周期溯源机制等，来切实保护数据生命周期安全。

2.2 风险视角下，安全隐患剧增，数据泄露频繁

（一） 内外部威胁共同造成安全隐忧

数据价值越来越受重视的同时，针对数据的攻击、违规行为也愈演愈烈。调查显示，除了黑客攻击，有内部人员参与的信息贩卖、共享第三方的违规泄露事件也层出不穷，约三分之二的安全威胁是从组织内部发起的。可见，在保证应用正常运行的前提下，如何及时发现和终止内部威胁，杜绝信息泄露的可能性，也是数据安全保护的重要问题。

（二） 终端环境不可控带来安全威胁

以智能手机为代表的轻量级客户端迅速普及，带来了移动办公的热潮，用户也越来越倾向于通过轻量级客户端访问数据和获取服务。据《中国移动互联网 2018 年度报告》中显示，中国移动互联网用户数高达 11.3 亿，移动社交、移动视频、移动购物、系统工具和金融支付成为移动端 5 大行业。但由于轻量级设备类型多样，安全能力相对弱，用户缺乏对恶意软件的防范意识，使得移动客户端的安全环境不可控，带来安全威胁。

此外，在万物互联时代，无人机、智能电视、智能音箱、智能摄像头、智能穿戴设备、智能医疗设备等物联设备终端也大量联网。但当前智能物联设备的安全能力都相对较弱，存在可被攻击者利用的安全漏洞。这也导致数据安全敞口极速扩大，数据安全风险严重加剧。

（三） 云计算模式下安全问题滋生

云计算模式减轻了企业和组织的运维压力，同时也带来了新的数

据安全问题。首先，由于云计算模式自身的特点，使得数据容易受到各种内外部攻击，包括隔离机制不健全导致的数据泄露、虚拟安全漏洞导致系统权限被盗、网络传输中遭遇数据篡改、集群配置漏洞导致数据被窃等。其次，云计算模式下，数据脱离企业和组织控制范围之外，企业和组织只能依赖于云服务商提供运行状态监控和审计信息，难以确认数据的安全性和可靠性。

2.3 合规视角下，政策要求明确，保护场景复杂

随着网络安全战略地位的上升和国家大数据战略的加快实施，我国推出了一系列法律法规和相关标准对数据安全保护，尤其是公民个人信息保护，进行规范和管理。

2017 年 6 月 1 日，《中华人民共和国网络安全法》正式实施，将个人信息保护列入法条，严格规定了用户信息收集、使用的保密和防泄漏原则，为网络安全工作提供了切实的法律保障。

为保护个人信息安全，同时促进数据的共享使用，2017 年 8 月，全国信息安全标准化技术委员会发布了《信息安全技术 个人信息去标识化指南(征求意见稿)》，为个人信息使用和传播提供了合规指导。

2018 年 5 月 1 日，国家标准《信息安全技术 个人信息安全规范》实施。该标准规范了个人信息控制者在收集、保存、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，以保障个人的合法权益和社会公共利益。

2018 年 6 月 27 日，公安部发布《网络安全等级保护条例（征求意见稿)》，要求落实数据分类、重要数据备份和加密等措施，防止个

人信息泄露、损毁、篡改、窃取、丢失和滥用，保障数据生命周期安全等。

2018 年 11 月 30 日，公安部网络安全保卫局发布《互联网个人信息安全保护指引（征求意见稿）》，规定了个人信息安全保护的安全管理机制、安全技术措施和业务流程的安全，以指导个人信息持有者在个人信息生命周期处理过程中开展安全保护工作。

欧盟《通用数据保护条例》（GDPR）也于 2018 年 5 月正式实施，该条例约束任何在欧盟境内设有业务机构的组织，以及任何收集、传输、保留或处理涉及到欧盟所有成员国内的个人信息的机构组织，对用户数据安全保护做出了详实、严格的规定，并对违法行为制定了高额的处罚条例。

此外，国际社会普遍对人工智能技术发展带来的数据安全风险表示担忧，并发出了在人工智能开发和应用中保护个人数据和隐私的倡议。美国信息技术产业理事会（ITI）于 2017 年 10 月发布《人工智能政策原则》报告，报告指出数据和网络安全是人工智能成功不可或缺的一部分，人工智能系统应使用工具以尽可能保护个人身份信息。2018 年 6 月，谷歌发布人工智能使用七原则，把隐私保护原则纳入 AI 技术的开发和使用中。在上海举办的 2018 年世界人工智能大会上，安全高端对话专家组发布《人工智能安全发展上海倡议》，提出人工智能发展需要保障用户的数据安全，人工智能发展不得以牺牲用户隐私为代价。

以上法律、法规、标准和倡议的涌现表明，数据安全已经成为国际社会普遍关注的问题，数据安全立法成为网络空间博弈的重要组成

部分。数据安全，已经成为企业发展的达摩克利斯之剑。

基于以上背景和需求，我们提出了数据安全保障工程建设框架和完整解决方案，旨在为我国政企单位提升数据安全保障能力提供可行建议。

3 数据安全保障工程建设框架

3.1 数据安全保障工程建设思路

深入学习贯彻习近平总书记系列重要讲话精神和治国理政的新理念、新思想、新战略，深入理解政企数据安全治理的内涵和外延，明确**“数据问题是数字时代的问题，数据安全是网络空间的安全！”**，明确政企数据资产的国家属性、社会属性和安全属性，全面贯彻落实总体国家安全观和网络安全强国的重要战略部署，准确把握数据安全保障工程建设要求，聚焦政企数据安全保护过程中遇到的重点和难点问题，构建体系化的数据安全保障方案，全面提升政企人员能力、过程管控能力、技术支持能力和数据安全能力，提升政企运营执行的效率和效果。

3.2 数据生命周期安全

根据大数据环境下，数据在政企单位及相关组织的业务中的流转情况，定义数据生命周期各个阶段，提炼出大数据环境下，以数据为中心的相关数据安全过程体系。数据生命周期包括以下六个阶段：

数据采集：指在组织机构内部系统中新生成的数据，以及从外部收集数据的阶段。

数据传输：数据在组织机构内部从一个实体通过网络流动到另一个实体的阶段。

数据存储：指数据以任何数字格式进行物理存储或云存储的阶段。

数据处理：指组织机构在内部针对数据进行计算、分析、可视化等操作的阶段。

数据交换：指数据由组织机构与外部组织机构及个人交互的阶段。

数据销毁：指通过对数据及数据的存储介质通过相应的操作手段，使数据彻底消除且无法通过任何手段恢复的过程。

特定的数据所经历的生命周期由实际的业务场景所决定，并非所有的数据都会完整的经历六个阶段。（*备注：《信息安全技术 数据安全能力成熟度模型》*）

3.3 以数据为中心的安全

随着大数据、虚拟化、云计算技术的成熟，政企各单位及各组织开展大数据局、大数据平台建设，实现数据的大集中，也意味着风险大集中。这就要求处理好安全环境和保护对象的辨证关系，在提供数据服务（包括云服务）的过程中，须进行敏感数据分类、分级，划分安全边界并明确数据安全访问控制措施，实现“以数据为中心”的安全审计和保护才是关键。

以数据为中心的审计和保护包括：安全评估、动态监测和安全保护。具体包括：

数据安全策略：跟进业务数据流转过程，有效结合数据安全保护需求，结合自身环境进行整体设计，设计并明确各类数据的安全保护策略和控制措施。

数据发现与分类：数据资产发现，对业务数据进行识别和分类，根据业务属性及数据属性，进行分级管理。

用户监控和审计：对用户相关角色和访问权限进行评估，对操作行为进行安全监控和审计，如特权用户或特定数据库，发现违规和异常操作，记录相关操作日志并进行预警和审计。

行为分析和告警：识别用户业务操作行为，识别业务访问逻辑、端口、账户、位置等信息，建立安全基线和访问控制策略，通过分析有效发现业务逻辑和访问异常，能够进行风险预警和处置，有效降低业务数据安全风险。

攻击预防和阻断：能够有效发现网络攻击行为和安全威胁，进行态势感知、安全预警并给出安全处置建议，对敏感信息的违规外发或用户的异常行为能够进行有效阻断。

加密、标记、脱敏：使用数据加密、标记和脱敏等数据安全保护工具，能够应用到业务数据流转过程，并根据业务场景进行动态调整，能够与已有平台进行集成。

3.4 数据安全保障工程建设框架

数据已经成为政企核心资产和经济发展命脉，无论是在国家安全、经济发展、社会生活中已起到关键作用，因为数据的高价值所以也成为了攻击者的重要目标之一。

数据安全保障工程（Data Security Assurance Engineering，DSE）是面向攻击语境下，以数据为中心，从三大驱动出发，构建全方位的数据安全保障工程，实现数字空间、网络空间和物理空间全覆盖，保障数据生命周期安全，持续提升数据安全保障能力。数据安全保障工程建设重点包括：数据安全治理和数据安全管理。

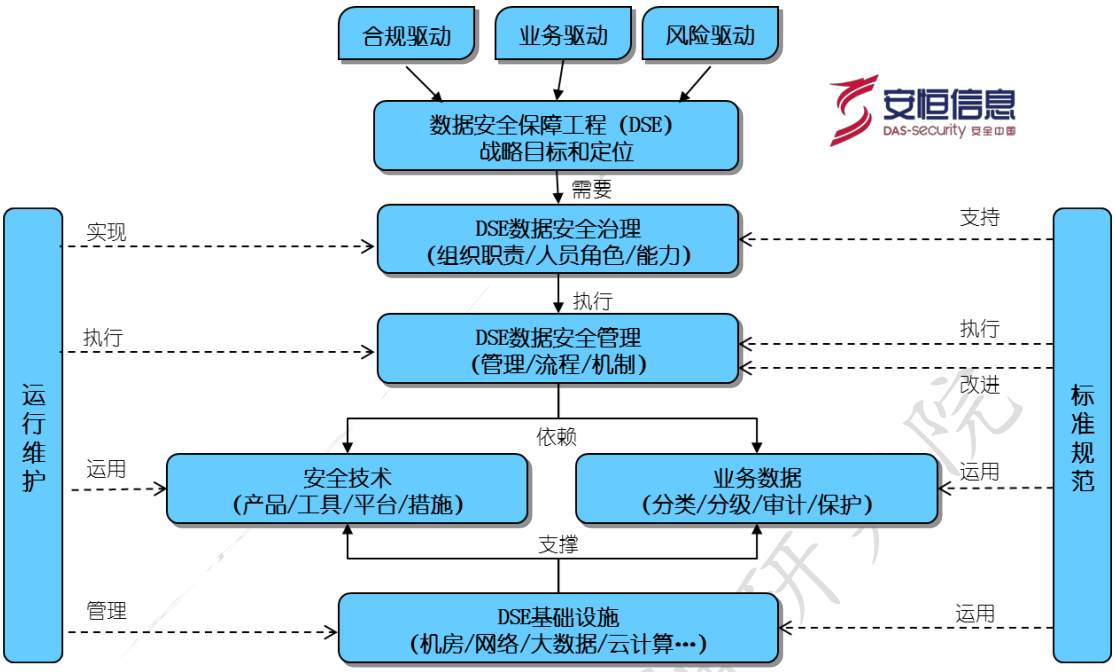

图 1 数据安全保障工程建设框架

3.5 数据安全能力成熟度模型

数据安全是一个体系化且复杂的系统工程，因此须持续提升组织数据安全保护能力，提升数据安全治理水平，持续提升数据安全保障成效。

数据安全能力成熟度模型借鉴了成熟度模型（CMM）的思想，明确组织机构在各数据安全领域应用具备的能力，数据安全能力维度包括：组织建立、制度流程、技术攻击和人员能力，共划分了五个能力成熟度级别，分别是：非正式执行、计划跟踪、充分定义、量化控制、持续优化。（*备注：参考《信息安全技术 数据安全能力成熟度模型》对级别的定义。*）

根据业界最佳实践，同时考虑政企在数据安全保障工程中的投入，以及业务数据可用性和保密性的平衡，建议数据安全能力成熟度最佳

合理区间是 3 级-4 级之间。

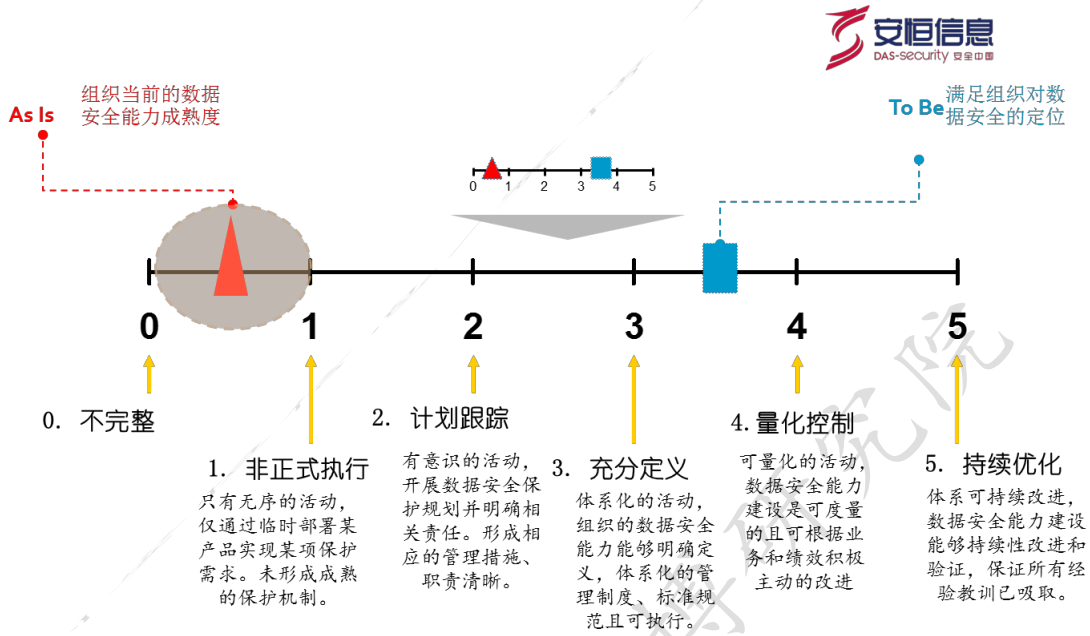

图 2 数据安全能力成熟度模型

4 数据安全治理体系架构设计

为了有效提升政企单位及相关组织的数据安全能力，我们参考业界最佳实践，并在大量研究成果和实践的基础上，进行了方法论的创新，设计并形成了一套适用于政企单位及相关组织可落地的数据安全治理架构，从数字空间、网络空间、物理空间形成了“三位一体”的新一代数据安全保护解决方案。

数字空间：数字空间主权。关注的是安全对抗和攻防实战，形成数字空间安全保障环，应对战略风险。

网络空间：业务数据安全以及数据在网络流转过程中的安全。关注的是数据全生命周期的安全保障，以数据为中心的安全，形成数据安全保障环，应对运营风险。

物理空间：支持业务运行和数据全生命周期的网络和基础设施。关注的是满足风险管控策略下的基础安全防护和安全运行维护，形成基础安全保障环，应对战术风险。

4.1 总体架构设计

数据安全保障工程建设应根据政企单位及相关组织的数据安全保护对象，遵从国家法律法规的合规性要求、业务安全需要和安全风险管治需求三个方面。从**数字空间、网络空间、物理空间**的风险管治角度进行体系化的设计和保障，建设并形成“以数据为核心”覆盖数据生命周期安全的**基础安全保障环、数据安全保障环和数字空间保障环**。因此，数据安全保障工程不仅需要考虑基于最佳实践的安全防范，更

加需要维护**面向攻击语境下的数字空间主权**，需要识别、分析、评估、处置和监测攻击语境下的风险。

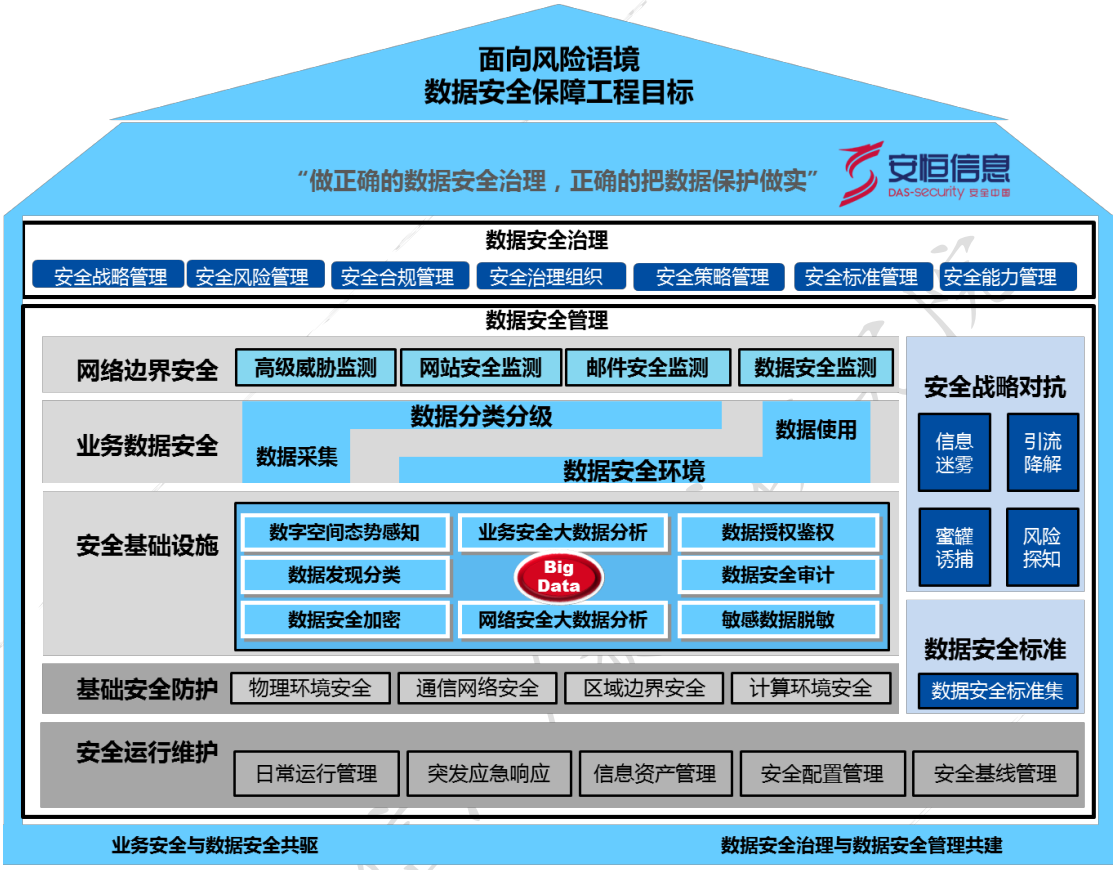

图 3 数据安全治理体系架构图

4.2 数据安全治理

数据安全治理：做正确的事！

在风险语境下为政企制订一套以业务安全为驱动，以业务数据为核心，支撑业务发展战略的政企数据安全治理方法论和体系框架，建立数据安全治理的组织，制订安全治理策略，满足合规性要求，规范数据安全标准，持续提升数据安全保障能力。实现以信息化为载体的数据生命周期安全，降低网络攻击、敏感数据外泄等数据安全问题给政企带来的风险。

数据安全治理是数据安全治理体系的重要组成部分。主要包括：安全治理组织、安全战略管理、安全风险管理、安全合规管理、安全策略管理、安全标准管理、安全能力管理。

4.3 数据安全管理

数据安全管理：正确的做事！

数据安全管理的核心是有效执行并实现组织（P）、过程（P）、技术（T）、数据（D）、智能（I）五大能力建设。落实数据安全保护团队，明确责任和边界，形成有效的数据安全保护过程机制，以及配套的制度、标准、流程、表单，逐步形成配套的工具、产品、系统、平台等安全措施，科学、系统的开展数据分类、分级工作，根据业务数据属性进行安全保护策略的制定和安全措施的择选，通过自动化、智能化手段持续提升安全保障和安全运行的效率和效果。

数据安全管理是数据安全治理体系的重要组成部分。主要包括七个部分内容：安全战略对抗、网络边界安全、业务数据安全、安全基础设施、基础安全防护、数据安全标准和安全运行维护。

- **安全战略对抗：**风险探知、蜜罐诱捕、引流降解、信息迷雾。
- **网络边界安全：**高级威胁监测、数据安全监测、网站安全监测、邮件安全监测。
- **业务数据安全：**数据导入过程的分类分级、数据使用过程的安全环境。
- **安全基础设施：**数据发现分类、数据授权鉴权、数据安全加密、数据安全审计、敏感数据脱敏、业务安全大数据分析、网络安

全大数据分析、数字空间态势感知。

- **基础设施安全：**物理环境安全、通信网络安全、区域边界安全、计算环境安全。
- **数据安全标准：**元数据标准、分类分级标准、数据预处理标准、数据组织标准等。
- **安全运行维护：**日常运行管理、突发应急响应、信息资产管理、安全配置管理、安全基线管理。

5 数据安全工程建设解决方案

5.1 建立数字空间保障环，应对战略风险

5.1.1 数据安全治理

数据安全治理以专门的治理组织为依托，以安全战略为指导，以安全风险、安全合规和安全标准为依据，制定和落实安全策略，提升安全能力，对安全管理过程进行评估、指导和监督，并不断优化整个治理过程。数据安全治理的过程并不限于静态、局部的安全管理策略和技术，而是以数据为中心设计和实施安全保护措施，以数据安全能力成熟度为抓手，能够更好地应对目前开放、复杂的数据生态环境。

- **安全治理组织：**成立专门的数据安全治理领导组织。数据安全治理组织负责制定和管理整体的数据安全治理战略和重要策略，对数据安全管理活动进行指导、评估和监督，并征求业务部门的需求和建议，推动落实具体的安全策略、规范和流程。
- **安全战略管理：**企业的安全战略应与企业的发展战略保持一致，兼顾数据安全和数据使用的需求。在数据安全治理过程中，需贯彻和落实企业的安全战略，并根据企业发展方向及时调整安全战略，调整安全治理侧重点。
- **安全风险管理：**为适应开放环境中数据安全风险的多变性，数据安全治理过程中需前瞻性地预测业务中可能遇到的安全问题，评估其风险，并设计对应的安全策略。随着业务的不断发展，也应不断地对安全现状进行评估，持续完善安全风险管理

过程。

- **安全合规管理：**安全合规管理通过各项管理制度与措施降低信息安全风险。在此过程中，需明确和落实相关的法律、法规和标准的要求，建立制度化、体系化、规范化的合规管理机制，对安全风险进行控制。
- **安全策略管理：**随着业务、环境、合规要求的不断变化，数据安全策略也需不断调整，以保证数据安全可用的目标。数据安全治理过程需对安全策略进行管理，并在数据生命周期内维护和落实安全策略。
- **安全标准管理：**数据安全治理过程应遵循一套覆盖数据生命周期的安全标准，通过安全标准管理对数据安全治理活动进行规范和指导，从而保证数据安全治理过程标准化和一致性。
- **安全能力管理：**安全能力是组织提升数据安全保护能力的核心，是应对安全威胁、分析安全事件、进行响应处置的重要支撑。在数据安全治理过程中，需根据组织建设、团队配置、人员角色和自身业务需求，加强安全能力建设，提高抵抗风险和风险管控能力，保证业务数据安全和业务稳定运行。

5.1.2 数据安全标准

数据安全标准是数据安全治理的重要依据，在业务、技术和管理方面为数据安全治理提供支持，能够有效提升业务规范性，提升数据安全质量、提高安全治理效率。在治理过程应制定和遵循的标准包括：元数据管理规范、数据质量管理规范、数据安全管理规范和对应的流程等。

- **元数据管理：**明确了技术元数据、业务元数据和管理元数据的内容、格式等信息，为企业数据资源的管理和应用奠定基础。元数据管理规范帮助企业理解元数据管理需求，建立开发和维护元数据标准的体系，促进元数据的开发、使用和分析，实现企业的数据溯源、资产发现等安全需求。
- **数据质量管理：**明确了数据的完整性、一致性、准确性、时效性等指标，是衡量数据质量的重要依据。数据质量管理规范帮助企业建立数据质量意识，明确数据质量需求，并以规范为准绳评估和分析数据质量，对数据质量进行持续监督和改善。良好的数据质量体系能够帮助企业更好地开发和使用大数据，提升数据价值。
- **数据安全管理：**明确了数据规划、开发和执行安全政策与措施等相关过程的细则，结合数据安全的技术手段来保证数据生命周期安全。数据安全管理规范应包括数据获取安全、数据脱敏、身份认证、角色授权、审计等方面的要求，有效规避业务过程中存在的数据安全隐患。

5.1.3 安全战略对抗

融合“主动防御和协同防御”技术，打造持续放心、互联互通、安全可控的数据安全环境，持续增强抗“扰乱、降解、欺骗”的安全保障能力，提升数据安全保障和对抗能力。

- **蜜罐诱捕：**在内外部署多个蜜罐节点，通过暴露出的漏洞引诱攻击者进行攻击，记录并学习攻击技巧，捕获恶意代码并进行分析，提升安全防护能力。

- **信息迷雾：**模拟正常业务系统和业务数据，部署高交互式仿真信息系统，扰乱攻击者的攻击对象，迷惑攻击对手的攻击方向，记录攻击手段和漏洞利用方式，让攻击者很难找到目标系统或数据，根据预警信息进行提前布控。
- **引流降解：**快速识别并发现 DDoS 攻击并进行引流和阻断，对 SYN Flood、UDP Flood、ICMP Flood、IGMP Flood、ACK Flood、DNS Query Flood、Ping Sweep 等流量型攻击；HTTP Proxy Flood、HTTP Get Flood、CC Proxy Flood、Connection Exhausted 等连接型攻击和 Smurf、Land-based、Teardrop、Fragment Flood、Red Code 等漏洞型攻击，并实时对这些攻击流量进行阻断处理，保障业务系统正常运行。
- **风险探知：**采用风险探知引擎并融合多种探测技术，对信息资产的风险进行快速探测和识别，主动收集安全设备、网络设备、主机、服务器以及工控设备的信息，发现目标存活情况、软硬件版本信息、漏洞信息等。

5.2 建立数据安全保障环，应对运营风险

5.2.1 网络边界安全

随着互联网技术的发展，来自互联网的安全威胁也越来越多，攻击也越来越频繁，数据泄露事件频繁发生。包括国家政治利益驱动的网络攻击行为，有组织的黑客群体经济利益驱动攻击行为，例如 NSA 方程式组织、Anonymous 黑客组织的攻击行为，雅虎公司因黑客入侵导致共 30 亿用户账号信息被窃取，到京东因内部恶意员工作案致使

共 50 亿条公民信息被泄露。

- **高级威胁监测：**情报驱动的高级威胁监测，帮助政企解决“未知安全威胁”的探测和感知，实现对 APT 和安全风险的事前发现，及时采取安全措施完成威胁的阻击和风险的蔓延，最大程度保证数据资产安全。
- **数据安全监测：**对网络数据进行捕获、深度分析、检测和预警，实现数据安全态势、分级规则管理、数据泄露溯源等。对内外网敏感数据泄露进行监控，对内网重要数据库操作行为进行审计和监控，对终端敏感信息进行监控。
- **网站安全监测：** 对网站漏洞、网页木马、网页防篡改、网站可用性进行全面监测。
- **邮件安全监测：**对邮件行为进行审计、安全分析和风险语境，快速发现邮箱暴力破解、退信分析、位置异常分析、Webmail 审计分析、指纹异常分析、疑似钓鱼邮件识别等，提高了邮件安全审计能力和精准度。

5.2.2 业务数据安全

数据分类分级是数据安全治理的基本任务，随着数据业务的发展和数据链的延伸，数据孤岛的困境被打破，数据安全环境也需要更多地数据安全联动措施来保护。因此，须在细粒度的数据分类分级基础之上，应用合理的数据安全措施，才能保证获得数据安全可用的治理效果。

- **数据分类分级：**数据分类与实际业务数据息息相关。通常可根据数据的内容、来源和用途对其进行分类。数据分级应充分考

虑到数据对国家安全、企业安全、用户安全的影响程度，以及是否涉及到重要数据和敏感数据等。应主要依据数据受到破坏后对国家、社会、公共利益以及企业和用户的合法权益所造成危害的程度来划分。

- **数据安全环境：**数据安全环境的建设和维护应坚持以数据为中心的建设思路，通过安全基础设施建立数据安全的基础，围绕数据生命周期各个阶段和业务的安全需求，重点进行相应的安全加固。通过整个数据业务系统的联动，为管理人员提供全局的安全视角，及时应对安全风险，保障运营安全。

5.2.3 安全基础设施

- **数据资产发现：**数据资产发现能够帮助政企自动发现数据资产，可通过自动和人工相结合的方式发现端口号、数据库类型等信息，对政企内部资产进行统计和梳理。数据资产发现还可以自动识别敏感数据，可通过预置的敏感数据类型和用户自定义的敏感数据特征自动识别数据资产中包含的敏感数据，并能持续对新增数据进行分析和发现，绘制数据地图。
- **数据授权鉴权：**数据授权鉴权可为大数据应用和服务提供安全保障。安全网关基于用户行为安全基线识别用户异常行为，基于用户身份、资源、操作和所处的动态环境评估风险，利用数据标签和用户风险等级对用户进行细粒度动态访问控制，从而防止数据泄露。
- **数据安全审计：**数据安全审计通过对安全事件、行为事件、漏洞扫描、状态监控等日志进行全面的标准化处理，自动学习和

改进安全基线行为模型，及时发现各种安全威胁、异常行为事件，确保政企业务的不间断安全运营。

- **数据安全加密：**数据安全加密提供对文件、数据库的加密能力。基于符合我国密码管理机构要求的加密算法，可自动对指定格式的文件进行加密或由用户自定义文件和目录进行加密。可指定不同粒度对数据库进行透明加解密，保证数据安全可用。
- **敏感数据脱敏：**敏感数据脱敏支持静态脱敏和动态脱敏两种模式。其中，业务数据离线处理过程应进行静态脱敏。根据业务数据处理要求，还应配置相应的数据脱敏支持服务组件或技术手段以支持应用过程中的动态脱敏。
- **业务安全大数据分析：**通过大数据安全解析技术和智能算法，进行业务数据采集存储，分析业务异常行为，对违规行为进行处置，通过识别业务访问逻辑、端口、账户、位置等信息，建立安全基线和访问控制策略，有效发现业务逻辑和访问异常，有效降低业务数据安全风险。
- **网络安全大数据分析：**对安全数据进行采集、解析、标准化和丰富化，通过威胁情报能够快速发现攻击和异常行为，能够形成全面的大数据安全解析、用户行为分析（UEBA）、安全预警、态势感知、追踪溯源，提升安全运行的效率和效果。
- **数字空间安全态势感知：**数字空间安全态势感知是“以数据为中心”的全局安全风险态势和指挥控制系统，呈现业务系统基础安全保护状况、资产地图、漏洞等；数据安全保护状况、数据流转、血缘、分布等；数字空间安全事件、处置响应、指挥

控制、安全预警等。

5.3 建立基础安全保障环，应对战术风险

5.3.1 基础安全防护

依据国家网络安全等级保护和关键信息基础设施安全保护等相关要求，以及个人信息安全规范、个人隐私保护、数据出境、数据交易服务等安全要求，明确政企在数据安全的建设需求和数据安全保护能力。并结合政企信息安全现状，形成体系化的规划方案，从而构建出基础安全保障技术框架。例如网络安全等级保护要求包含：物理环境、通信网络、区域边界、计算环境安全等。

5.3.2 安全运行维护

由于数据安全保障工程（DSE）的复杂性、专业性、可行性和可维护性，DSE 由规划、设计、建设，转为后期的安全运行维护均需要有较为专业的安全服务支持。因此需要从日常运行维护、突发应急响应、信息资产管理、安全配置管理、安全基线管理五个方面进行重点建设，形成一整套适用于政企数据安全保护各个层面的安全制度、流程以及运行维护作业计划和检查标准，使政企数据安全保障工作实现体系化、规范化、流程化，长期稳定的保障各业务系统安全运行。

- **日常运行维护：**系统日常维护、日常定检、介质管理、账号口令管理、防病毒管理、安全风险评估、安全加固等。
- **突发应急响应：**持续监控与事件处理、备份与恢复管理、应急响应与应急预案、重保等工作。

- **信息资产管理：**人员资产、数据资产、设备资产、软硬件资产等进行统一管理和维护。
- **安全配置管理：**网络设备、安全设备、主机、服务器、应用系统等安全配置、补丁、变更管理等。
- **安全基线管理：**根据网络设备、安全设备、终端、主机、服务器、应用系统的厂商、型号、部署位置、作用等明确安全基线并进行安全加固。明确安全红线，落实安全责任，做到“令行禁止”。

6 数据安全保障工程建设蓝图

图 4 数据安全保障工程建设蓝图(DSE)

数据安全治理给国家、政府、企业等组织带来很大困扰，如何有效开展数据安全治理工作是各界当前亟需解决的问题，数据安全问题不仅仅停留在违规层面，已经触犯了法律底线属于违法范畴。

数据安全问题需要各界同仁不断提高数据安全保护的意识，需要在组织（P）、过程（P）、技术（T）、数据（D）、智能（I）五个层面进行相应的资源保障

通过数据分类、分级、标签技术、动态脱敏、语法解析、同态加密、智能流量解析、智能协议解析、UEBA、机器学习、基于零信任的

数据安全网关等多方面的新技术突破和应用实践，数据安全保障工程建设力争为政企打造持续放心的数据安全保障体系提供有效抓手！