文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

# 企业数据安全治理与技术防护平台构建研究

何慧
中国航发中传机械有限公司
DOI:10.12238/acair.v2i4.10335

[摘　要] 本文探讨了企业数据安全治理与技术防护平台的构建,分析了企业数据安全面临的复杂挑战,提出了构建数据安全治理体系的思路,包括明确数据权属关系、加强数据安全能力建设、实施全生命周期保护等。同时,本文还介绍了技术防护平台的构建方法,包括基础设施安全、网络安全防护、应用安全防护和数据安全防护等方面。最后,本文强调了数据安全治理与技术防护平台的融合,以实现二者的有机结合,确保企业数据的安全性。
[关键词] 数据安全治理；技术防护平台；企业数据安全
中图分类号：R142　文献标识码：A

## Research on Enterprise Data Security Governance and Technology Protection Platform Construction

Hui He
China Aerospace Science and Technology Corporation (AVIC) Zhongtian Machinery Co., Ltd.
[Abstract] This article explores the construction of enterprise data security governance and technology protection platforms, analyzes the complex challenges faced by enterprise data security, and proposes ideas for building a data security governance system, including clarifying data ownership relationships, strengthening data security capacity building, and implementing full lifecycle protection. Meanwhile, this article also introduces the construction methods of the technology protection platform, including infrastructure security, network security protection, application security protection, and data security protection. Finally, this article emphasizes the integration of data security governance and technology protection platforms to achieve an organic combination of the two and ensure the security of enterprise data.
[Key words] Data security governance; Technical protection platform; Enterprise Data Security

## 引言

随着信息化技术的飞速发展,大数据已成为企业运营中不可或缺的重要资源。然而,随着数据价值的不断提升,数据安全威胁也日益严峻。近年来,国内外频繁发生的数据泄露事件,不仅损害了用户隐私,也给企业带来了巨大的经济损失和声誉风险。因此构建一套完善的企业数据安全治理体系和技术防护平台,已成为企业保障数据安全、实现可持续发展的关键。

## 1 企业数据安全治理的现状与挑战

在当今信息化高速发展的时代,企业数据安全治理面临着前所未有的复杂性和严峻性。数据安全风险的形成原因多样且复杂,这不仅考验着企业的技术防范能力,更对企业的管理水平和员工的安全意识提出了高要求。

### 1.1数据安全风险成因复杂

企业数据安全风险的形成,其成因犹如一张错综复杂的网,既有来自外部的恶意攻击,也有源自内部的潜在威胁。外部攻击方面,黑客入侵、病毒传播等手段层出不穷,这些攻击往往具有高度的隐蔽性和破坏性,给企业的数据安全带来极大的挑战。而内部泄露同样不容忽视,员工疏忽大意、恶意泄露敏感信息,或是系统存在漏洞被不法分子利用,都可能成为数据泄露的导火索。随着云计算、物联网等新技术和新模式的不断涌现,数据交互的频率和范围都在不断扩大,这无疑增加了数据泄露的风险。这些新技术虽然为企业带来了便捷和高效,但同时也为数据安全治理带来了新的课题和考验。

### 1.2威胁范围全域覆盖

大数据安全威胁的触角已经渗透到了数据生产、交互和消费等大数据产业链的每一个环节。无论是数据源的提供者、大数据加工平台的提供者,还是大数据分析服务的提供者,这些主体在数据处理的过程中,都可能成为数据泄露的源头。数据安全治理的覆盖面必须广泛而深入,从数据采集的源头开始,到数据存储、传输、处理,再到最终的销毁,每一个环节都不能有丝毫

Copyright © This work is licensed under a Commons Attibution-Non Commercial 4.0 International License.

的疏忽和遗漏。只有建立起全方位、多层次的数据安全防护体系,才能有效地抵御来自各方的数据安全威胁。

1.3事件影响重大深远

数据泄露事件一旦发生,其影响将是深远而广泛的。对于用户而言,个人隐私的泄露可能带来无尽的困扰和损失;而对于企业而言,数据泄露则可能导致客户流失、信誉受损,甚至面临法律诉讼和巨额罚款的严重后果。企业数据安全治理不仅关乎用户隐私的保护,更关乎企业的生存与发展。企业必须高度重视数据安全治理工作,不断提升自身的数据安全防护能力,以确保企业的稳健发展和用户的合法权益。

## 2 企业数据安全治理体系的构建

2.1明确数据权属关系

企业数据安全治理的首要任务是明确数据权属关系。企业应建立数据分类分级制度,对不同类型、不同级别的数据采取不同的保护措施。企业应明确数据的采集、存储、传输、处理、交换和销毁等各个环节的责任主体,确保数据在各个环节都得到有效的保护。

2.2加强数据安全能力建设

企业应从制度流程、人员能力、组织建设和技术工具等方面加强数据安全能力建设。制度流程方面,企业应制定完善的数据安全管理制度和操作规程,确保数据安全管理的规范化和标准化。人员能力方面,企业应加强对员工的数据安全培训,提高员工的数据安全意识和技能水平。组织建设方面,企业应成立专门的数据安全管理机构,负责数据安全管理的组织、协调和监督工作。技术工具方面,企业应采用先进的数据安全技术工具,如数据加密、数据脱敏、数据备份等,提高数据的安全防护能力。

2.3实施全生命周期保护

企业数据安全治理应贯穿数据的全生命周期,从数据采集、存储、传输、处理到销毁,每一个环节都需要得到有效的保护。在数据采集环节,企业应确保数据的合法性和准确性；在数据存储环节,企业应采用安全可靠的存储设备和存储技术,确保数据的安全存储；在数据传输环节,企业应采用加密传输技术,确保数据在传输过程中的安全性；在数据处理环节,企业应加强对数据处理过程的监控和管理,确保数据处理的安全性和合规性；在数据销毁环节,企业应确保数据的彻底销毁,防止数据泄露和滥用。

## 3 技术防护平台的构建

在数据安全防护的体系中,技术防护平台的构建起着至关重要的作用。它不仅能够提供有效的安全保障,还能为数据的全生命周期管理提供坚实的支撑。以下是对技术防护平台构建中各个关键环节的详细解析。

3.1基础设施安全

技术防护平台的基础设施安全是整个数据安全体系的基础。大数据服务器作为数据存储和处理的中心,其安全性直接关系到数据的完整性和保密性。为了确保大数据服务器的安全,企业需要采取一系列的安全措施。服务器之间的认证以及客户端到服务器的认证是必不可少的,这可以确保只有合法的用户或设备才能访问服务器。用户访问级别控制也是关键,它可以根据用户的身份和权限来限制其对数据的访问范围,从而防止数据的非法访问和泄露。除了服务器本身的安全,企业还应加强对数据中心的物理安全防护。数据中心作为大数据存储和处理的核心场所,其安全性同样至关重要。企业应设置门禁系统,确保只有授权人员才能进入数据中心。同时运用UPS系统(不间断电源系统)可以保证在电力故障时数据中心的正常运行。进行视频监控也是必要的,它可以实时监控数据中心的安全状况,及时发现并处理潜在的安全威胁。

3.2网络安全防护

网络安全防护是技术防护平台的重要组成部分。随着网络技术的不断发展,网络攻击手段也层出不穷。为了确保网络的安全运行,企业需要采用多种技术手段进行防护。防火墙作为网络安全的第一道防线,可以阻止未经授权的访问和攻击。漏洞扫描可以帮助企业及时发现并修复网络系统中的安全漏洞,防止黑客利用这些漏洞进行攻击。DDOS防护也是必不可少的,它可以有效防止分布式拒绝服务攻击对网络造成的破坏。

除了技术手段的防护,企业还应加强对网络边界的防护。网络边界是内外网络之间的分界线,也是黑客攻击的重点。企业应设置严格的访问控制策略,防止外部攻击者通过非法手段进入内部网络。对于恶意内部工作人员的跨越式攻击,企业也应采取相应的技术手段进行防范和监控。用户协议隔离等技术手段可以实现内网和外网的资源限制,确保网络的安全隔离。

3.3应用安全防护

应用安全防护是技术防护平台的关键环节。随着企业信息化程度的不断提高,应用系统已经成为企业运营和管理的重要工具。然而应用系统也面临着各种安全威胁。为了确保应用系统的安全,企业需要采取一系列的安全防护措施。防止ATP攻击(高级持续性威胁)是必不可少的。ATP攻击通常具有隐蔽性强、持续时间长等特点,企业需要加强监测和预警机制,及时发现并处置ATP攻击。WAF(Web应用防火墙)可以保护Web应用免受常见的网络攻击,如SQL注入、跨站脚本等。SDLC(软件开发生命周期)安全管理也是关键,它可以在软件开发的各个阶段融入安全考虑,确保软件产品的安全性。

除了安全防护措施外,企业还应加强对应用系统的访问控制。只有授权用户才能访问应用系统,这可以确保数据的合法使用并防止数据的非法泄露。数据加密技术也是必不可少的。通过对数据进行加密处理,可以确保数据在应用系统中的安全性,即使数据被非法获取也无法被轻易解密。

3.4数据安全防护

数据安全防护是技术防护平台的核心任务。数据作为企业的核心资产之一,其安全性直接关系到企业的生存和发展。为了确保数据的安全性,企业需要采用多种技术手段进行防护。数据脱敏技术可以在不影响数据分析结果的前提下对数据进行处理,降低数据泄露的风险。策略化数据抽取和集成可以帮助企业实


Copyright © This work is licensed under a Commons Attibution-Non Commercial 4.0 International License.

现数据的规范化和统一管理，提高数据的安全性和可用性。数据加密技术也是必不可少的。通过对数据进行加密处理，可以确保数据在存储、传输和处理过程中的安全性。

除了技术手段的防护外，企业还应加强对数据的备份和恢复管理。数据的备份和恢复是确保数据可靠性和可用性的重要手段。企业应制定完善的备份策略，定期对数据进行备份，并测试备份数据的恢复能力。对于关键业务数据，企业还应采用冗余备份和异地备份等措施，确保在灾难发生时能够迅速恢复数据并恢复业务运行。

此外企业还应建立数据安全监测和预警机制。通过实时监测数据的安全状况并及时发现和处置数据安全事件，可以最大程度地降低数据泄露和损坏的风险。企业还应定期对数据安全体系进行评估和改进，确保数据安全体系的持续有效性和适应性。

## 4 数据安全治理与技术防护平台的融合

数据安全治理与技术防护平台是相互依存、相互促进的。数据安全治理为技术防护平台提供了指导和方向，而技术防护平台则为数据安全治理提供了有力的支撑和保障。企业应将数据安全治理与技术防护平台紧密结合，实现二者的有机融合。

4.1制定数据安全策略

在制定数据安全策略方面，企业应根据数据安全治理的要求，制定一套完善的数据安全策略。这套策略应涵盖数据的分类分级、采集、存储、传输、处理和销毁等各个环节的安全要求，确保数据在生命周期的每一个阶段都能得到充分的保护。同时，数据安全策略还应明确数据安全事件的处置流程，包括事件的发现、报告、调查、处理和后续改进等环节，以确保在数据安全事件发生时能够迅速响应、有效处置。在制定数据安全策略时，企业应充分考虑技术的可行性和管理的可操作性，确保策略既能够切实保障数据安全，又能够符合企业的实际情况和运营需求。

4.2加强数据安全监测

加强数据安全监测是数据安全治理与技术防护平台融合的重要环节。企业应建立一套完善的数据安全监测机制，实时监测数据的安全状态。这种监测应涵盖数据的访问记录、修改记录、异常行为等方面，以便及时发现和处置潜在的数据安全威胁。通过数据安全监测，企业可以实时掌握数据的安全状况，及时发现并处置数据安全事件，从而确保数据的安全性。同时，数据安全监测还可以为企业提供数据安全的趋势分析和预警服务，帮助企业提前发现潜在的数据安全风险，并采取相应的预防措施。

4.3完善数据安全应急响应机制

完善数据安全应急响应机制也是数据安全治理与技术防护平台融合的关键一环。企业应建立一套完善的数据安全应急预案，明确数据安全事件的处置流程、处置措施和责任主体等内容。在数据安全事件发生时，企业能够迅速启动应急预案，按照预案的指示进行处置，从而有效控制事态的发展，减少损失。同时数据安全应急预案还应包括后续的改进措施和教训总结等内容，以便企业能够从中吸取教训，不断完善数据安全管理体系和技术防护平台。

## 5 结束语

随着信息化技术的不断发展，数据安全已成为企业运营中不可或缺的重要资源。然而数据安全威胁也日益严峻，企业数据安全治理与技术防护平台的构建已成为企业保障数据安全、实现可持续发展的关键。本文通过分析企业数据安全治理的现状与挑战，提出了企业数据安全治理体系的构建思路和技术防护平台的构建方法。本文还强调了数据安全治理与技术防护平台的融合，以实现二者的有机融合。希望本文的研究能够为企业数据安全治理与技术防护平台的构建提供参考和借鉴。

## [参考文献]

[1]何航.企业数据安全合规治理的关键问题与纾解[J].贵州社会科学,2022,394(10):126-133.

[2]高磊,赵章界,宋劲松,等.大数据应用中的数据安全治理技术与实践[J].信息安全研究,2022,8(4):326-332.

[3]都业涛.大数据背景下数据治理的网络安全措施[J].数字通信世界,2022(10):194-196.

[4]许杰,张锋军,陈捷,等.面向大数据环境下的数据安全治理技术[J].通信技术,2021,54(12):2659-2665.

[5]朱琴琴.基于信息化的企业数据安全管理体系构建研究[J].电脑知识与技术,2024,20(17):95-97.

## 作者简介：

何慧(1981--),女,汉族,湖南省益阳市人,本科,中级,工程师,研究方向:(工作领域):数据管理,信息安全,架构设计,平台建设。

Copyright © This work is licensed under a Commons Attibution-Non Commercial 4.0 International License.