主 编 蒋 平
副主编 孙银霞

网络与信息安全问题研究

数据安全与取证
网络攻击与防范
下一代网络风险与对策
信息安全保密
个人信息保护

社会科学文献出版社
SOCIAL SCIENCES ACADEMIC PRESS(CHINA)

网络与信息安全问题研究

主 编 蒋 平
副主编 孙银霞

网络与信息安全问题研究

社会科学文献出版社
SOCIAL SCIENCES ACADEMIC PRESS (CHINA)

图书在版编目(CIP)数据

网络与信息安全问题研究 / 蒋平主编. --北京：
社会科学文献出版社，2018.1
ISBN 978-7-5201-1738-8

Ⅰ.①网… Ⅱ.①蒋… Ⅲ.①计算机网络-信息安全
-研究 Ⅳ.①TP393.08

中国版本图书馆 CIP 数据核字(2017)第 273159 号

网络与信息安全问题研究

主　　编 / 蒋　平
副 主 编 / 孙银霞

出 版 人 / 谢寿光
项目统筹 / 许春山
责任编辑 / 王珊珊

出　　版 / 社会科学文献出版社 · 教育分社(010) 59367278
地址：北京市北三环中路甲 29 号院华龙大厦　邮编：100029
网址：www.ssap.com.cn
发　　行 / 市场营销中心 (010) 59367081　59367018
印　　装 / 北京季蜂印刷有限公司

规　　格 / 开 本：787mm × 1092mm　1/16
印 张：16.75　字 数：211 千字
版　　次 / 2018 年 1 月第 1 版　2018 年 1 月第 1 次印刷
书　　号 / ISBN 978-7-5201-1738-8
定　　价 / 48.00 元

本书如有印装质量问题　　367028) 联系

序

随着社会信息化的发展，以网络为平台的信息基础设施对整个社会的运行和发展起着越来越重要的作用。同时，网络空间面临的威胁也日益突出。网络上机密信息的泄露事件已屡见不鲜，以非法牟利为目的、利用计算机网络进行犯罪已经形成了一条黑色的地下产业链，对社会稳定、经济发展构成了严重的威胁。没有网络安全就没有国家安全，加强网络安全已经成为国家安全战略的重要组成部分。

研究小组相关作者自 1995 年以来，围绕网络安全、信息保密等方面展开了多方位的研究，相继开展了一系列讲座，并发表了一系列文章，现结集出版，意在向广大研究者和学术界提供一些目录性、连续性和渐进式的资料参考，也从一个侧面反映我国在相关领域的研究缩影。全书包括五部分内容：数据安全与取证、网络攻击与防范、下一代网络风险与对策、信息安全保密、个人信息保护。其中有些文章发表时间很早，观点略显陈旧，资料略显单薄，方法略显单一，但为了保持原貌，本次结集未做较大修改，请专家学者和各界人士批评指正。

编者

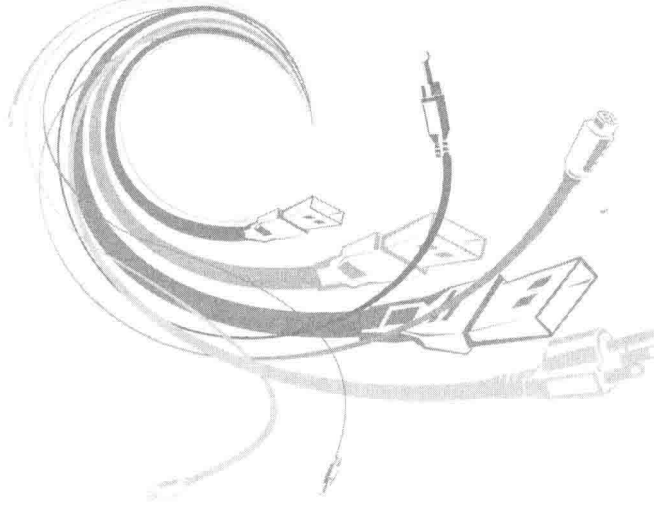
2017 年 6 月

目录

数据安全与取证

这部分内容整理了有关数据安全与取证的研究成果，共收集了两篇文章：《数据集中与安全》《数字取证技术研究的现状和展望》。

第一篇文章介绍了数据集中的特点、优势，探讨了数据集中的安全隐患和安全对策。第二篇文章介绍了数字取证的概念以及取证技术的研究范围，详细阐述了取证技术的研究进展，并对取证工具的研制以及相关的行业标准和规范进行了分析研究。



数据集中与安全

计算机信息管理系统的发展经历了集中－分布－再集中的发展阶段，二十世纪七八十年代，美国等发达国家在涉及全国性的基础建设领域、政府军队及各个行业部门建设信息系统时即采用这种集中模式，如国家犯罪信息中心（NCIC）等。二十世纪八十年代，由于个人计算机和网络的发展，一度出现了以客户工作站为中心的应用模式，二十世纪九十年代，随着中心服务器技术、数据库技术、网络技术、互联网技术等飞速发展，越来越多的行业意识到数据集中对于节约投资、方便管理、提高业务工作效率的重要意义。二十世纪九十年代末，我国银行业在信息化建设中率先采取数据大集中模式。近年来，这种信息化建设模式逐渐得到了整个 IT 行业的认可，与之相适应，数据大集中技术飞速发展，如存储区域网络技术（SAN）、集群技术（CLUSTER）及并行数据库技术等已非常成熟，系统建设成本也大大降低，我国很多行业和部门都相继开展了数据大集中的项目建设。但技术的发展往往是一把双刃剑，数据大集中在给信息化建设带来许多突破和活力的同时，也潜藏着一些问题，最为突出的是如何确保数据安全。本文就此问题发表一孔之见。

一　数据集中的特点与优势

（1）节约建设经费，降低维护成本。分散建设造成了重复建

设、重复投资，而且随着对系统性能要求、安全性要求的不断提升，以及系统的不断升级换代，整个信息化建设在硬件设备方面的投资是相当惊人的。而数据集中虽然短时间内投资较大，但避免了重复建设，同时系统建设一步到位，数据备份、系统容灾等方面的设施完善，整个系统的性能和安全性大大提高，与相同档次的分散建设相比建设经费大大减少。同时，由于数据集中，管理人员和维护力量等可集中安排，避免搞小而全，而增加管理人员数量及维护经费开支等。

（2）为信息共享、数据整合和高水平、深层次的应用创造了便利条件。数据集中打破了各部门对数据的封锁，信息的共享不再受到业务部门本位主义的限制；数据的集中保证了数据的高度一致性，各种数据操作非常方便灵活。这些条件都非常有利于开展数据整合和高水平、深层次的信息化应用。

（3）提高了系统的可靠性和安全性。系统安全建设是信息化建设的一个重要组成部分，涉及网络安全、操作系统安全、数据安全和管理制度等方面，其中数据安全建设是核心。数据集中处理有利于制定各种安全管理制度，便于系统维护和系统访问控制，符合提高系统安全性的要求。同时数据集中便于实施相应的数据备份和系统容灾方案，数据安全性大大提升。

（4）减缓了各部门对技术人员的需求压力，业务部门可以集中精力完成自己的业务工作。目前，各行各业及其内部各业务部门对信息化工作都非常重视，并取得了一定的成效，但还存在着一定的差距。从整体来看，信息技术人员的供需矛盾还非常突出，采用数据集中策略可以充分发挥技术部门的优势，减缓了各业务部门对技术人员的需求压力，业务部门可以集中精力完成自己的业务工作。

（5）有利于开展数据挖掘和网上统计分析等工作。在现行数据分布存储的情况下，数据挖掘和网上统计分析很难开展，各基

层单位的统计报表基本上由手工填写，基层单位常常为填写报表伤透脑筋，而且也很难保证统计数据的准确性。数据集中保证了信息中心拥有最新最全面的数据，可以很方便地开展数据挖掘和网上统计分析。

（6）有利于适应管理和业务工作“扁平化”模式发展需要。为提高管理和业务工作效率，建立“扁平化”工作模式日益成为各行各业适应现代社会发展需要的一个重要目标，而实现数据集中，减少中间环节，正是以信息为中心的业务工作“扁平化”的重要支撑。

二　数据集中产生的问题和隐患

数据集中处理策略在带来许多优势的同时也产生了一些问题，造成了许多隐患。随着数据的大集中，信息技术风险大大增加，对技术、业务和生产运营的统一规范管理提出了更多更高的要求，对软件开发和系统运行的质量要求大大提高，对数据安全和灾备的保障要求更是刻不容缓。

（1）中心服务器的压力大大增加，对于数据量较大的单位，选用性能一般的服务器可能无法承担集中处理带来的压力。随着应用规模的扩大，对中心服务器的配置要求会越来越高。

（2）中心的网络压力大大增加，有可能造成网络的堵塞。随着今后应用规模的不断扩大，图像、视频等大数据传输将对网络产生压力，当所有的压力集中到中心这一点时，就可能造成中心的网络堵塞。

（3）中心数据库的压力大大增加，如果处理不当，有可能数据库性能骤减，甚至无法使用。由于数据量和并发用户数的骤然增加，中心数据库承担了巨大压力，因此如何保证中心数据库的处理性能至关重要。这就要求数据库管理人员能够根据要求在数

据库设计、维护方面尽量优化，提高性能，同时在应用模式上采用中间件技术和三层架构（即数据库服务器、应用服务器、客户工作站），实现负载均衡，提高并发处理能力。如果仍然使用原有的一些老应用系统，由于体系结构，如采用 Client/Server 二层体系结构，在大规模应用时会直接对数据库产生巨大压力，同时数据库服务器过于暴露，安全性受到影响。此外，数据库结构设计时使用不当的数据类型和存储方案也很可能导致数据库性能降低。

（4）对应用软件开发质量的要求大大提高，一些不成熟的应用软件可能对中心服务器的性能产生巨大影响，导致其他系统无法正常运行。多个应用在大集中数据库系统中运行，就很可能发生一个应用出现问题，其他的应用也就受到了影响。例如，如果某个应用系统在数据库设计时性能没有调整好，或者其应用程序的 SQL 语句没有注意优化，处理效率低，就可能造成整个数据库性能骤减，甚至无法使用。

（5）系统安全管理压力加大。安全的威胁主要来自以下几方面：①系统自身软硬件故障造成的不能正常工作和数据丢失。②自然灾害和客观环境的影响。③计算机病毒感染、恶意破坏和攻击。④信息保密需求，以及访问控制和管理。⑤内部人员滥用权利、越权访问机密信息或篡改数据。为此，信息中心的责任重大，数据丢失、涉密信息外泄或数据被非法修改可能导致责任追究。信息中心必须加强安全技术保障，规范管理制度，强化督促检查，严禁无关人员随意出入中心机房，加强物理运行环境监控，坚决防止火灾等灾难发生。

三　数据集中的安全对策

针对上述存在的问题，本文提出相应对策以消除或减轻问题

的危害：

（1）在选择服务器时，对服务器的性能要求进行较好的测算，选择满足当前和今后一段时期应用要求的服务器，可以采用集群技术，达到热切换和负载均衡的要求。

（2）为避免网络压力过大，一方面在信息中心需要提高网络交换能力，可以通过建设冗余的具有第三层交换能力的局域网核心，主要服务器主机、存储设备通过光纤千兆网卡连入中心交换机，保证核心系统无单点故障；另一方面，可以考虑建立分中心，将视频等应用分流，减轻网络压力，同时两个中心可以互做容灾备份。

（3）做好数据库的性能监视和性能调整，注意应用程序在操作数据库时的优化工作。

（4）注重软件的开发质量，增加开发测试平台，通过对应用系统的整合减少应用系统，对每个应用系统尽可能先采用单独服务器进行测试运行，待相对稳定成熟后，再移入中心服务器。

（5）对老系统进行改造，通过采用中间件技术和三层体系架构减轻数据库服务器的压力并提升数据库的安全性，同时将原有老系统数据库设计中可能影响性能的数据定义进行升级，进行必要的表空间存储调整，提升数据库的性能。

（6）加强安全管理，建立安全管理保障模型。系统安全管理模型如图 1 所示。

图 1　系统安全管理模型

系统的技术安全主要是针对系统本身的物理的、技术性的安全手段和措施。安全管理是各项安全措施能够有效发挥作用的保证。安全管理的内容可以分成安全技术管理和安全制度管理两部分。安全技术管理包括安全服务的激活和关闭、安全相关参数的分发与更新（如密钥管理等）、安全相关事件的收集与告警等。在安全管理中，安全政策是制定安全方案和各项管理制度的依据。安全政策是有一定的生命周期的，一般要经历风险分析、安全政策制定、安全方案和管理制度的实施、安全审计和评估四个阶段。为此重点要做好以下几方面的安全防范和保障：

（a）做好系统的安全管理。使用防病毒系统和入侵监测系统，提升系统的安全性，并做好对操作系统、应用系统和数据的备份工作及有关系统安全补丁工作。

（b）做好数据库安全管理。为应用系统创建用户时要合理授权，日常操作数据的用户只能拥有满足其工作需要的权限而不能拥有过高权限（如删除工作表的权限等）。如使用 Oracle 数据库时，系统缺省的 internal、sys、system 等用户的口令在系统安装后必须立即修改。数据库管理员必须具备全面的数据库管理知识和细致负责的工作作风，做好数据库的日常管理工作，并制定完善的数据备份策略，切实保证数据的安全。

（c）加强数据访问的审计，监控可疑行为，建立不可抵赖性的数据访问日志，在发现问题时有据可查。建立数据丢失、涉密信息外泄或数据被非法修改责任追究制。

（d）加强系统访问用户和角色的权限设置，建立基于 PKI 体系的安全认证中心。

（e）加强信息中心机房的安全管理，设立门禁、监控系统，防止无关人员进入，强化内部人员的责任感，建立和落实各项安全管理制度。

（f）严格数据备份制度，确保数据安全。通过磁带库每天进

行数据备份，或进行数据异地存放，实施系统及数据级容灾方案都可以将安全风险降低。每天进行磁带备份并将磁带存放在异地，可以保证在最糟糕的情况下一天前的数据得以保留；如果实施了容灾方案，如采用 SAN 存储阵列技术，实现底层数据镜像，可以将信息中心的数据同步复制到备份中心的阵列中，如果备份中心配备一定的主机设备，即便是在最糟糕的情况下，备份中心也可以很快接替信息中心的工作。

（g）合理调配和使用硬件系统资源。各个应用系统的数据库应当尽可能分开，即便是多个应用系统合用一台数据库服务器，也应当在这个服务器上建立多个数据库实例，各应用系统使用自己的数据库实例，同时数据库采用归档模式，根据备份策略进行日常数据备份。一旦出现数据被批量错误删除、修改的现象，可以根据备份数据和重做日志文件对该数据库进行恢复，将损失降至最低。

通过上面的分析可以看出，为减轻数据集中带来的风险和压力，在实施数据集中计划之前，我们必须很好地预见各种可能发生的情况，切实做好方案设计和人才培养；一旦实施了数据集中计划，必须切实落实好安全管理模型的各项工作，认真做好系统和数据的备份工作，不能有丝毫的麻痹和松懈思想；在条件允许的情况下，建立异地容灾备份中心也是降低风险的好办法，同时备份中心可以承担一部分应用，减轻信息中心的网络压力，信息中心和备份中心可以互做容灾备份。

四　结束语

数据集中代表了目前信息化发展的一种潮流和趋势，它为信息化建设带来了诸多便利，但我们也要清醒地看到：数据大集中给我们带来了巨大的风险和压力。如何预见到这些风险，并采取

相应对策规避或降低风险是每个信息主管人员的职责。通过前面的论述，我们可以看到：数据集中带来的安全问题涉及各个层面，必须制定完整的安全策略，加强安全技术保障系统建设，建立完善的安全管理运行保障机制，保持一支高素质的人才管理队伍，建立各项应急工作预案，健全各项安全管理规章制度，同时要清醒地认识到安全的相对性，必须把其当作一项长期性的艰巨任务来抓，根据各类技术应用的发展，及时加强和调整各项安全策略，确保数据集中后，各应用系统安全可靠地运行，充分发挥数据集中所带来的作用和优势。

参考文献

洪崎：《数据集中与数据挖掘》，《中国金融电脑》，2002 年第 10 期。

戚红：《分布与集中式数据库结构利弊分析及相应解决方案》，《计算机时代》，2002 年第 9 期。

张军平、沈安文：《一种高效安全的银行数据存储系统研究》，《三峡大学学报》（自然科学版），2002 年第 5 期。

胡维浩：《浅谈数据中心的安全运行管理》，《华南金融电脑》，2002 年第 10 期。

（作者：蒋平，本文原载于《中国公共安全》2003 年第 5 期）