

# Web服务 安全

马恒太 李鹏飞 颜学雄 洪志国 编著



电子工业出版社  
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY  
<http://www.phei.com.cn>

安全技术  
大系

# Web服务 安全

马恒太 李鹏飞 颜学雄 洪志国 编著

电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

## 内 容 简 介

Web 服务技术是最近几年迅速兴起的一种应用集成技术,而安全问题是影响该技术广泛应用的一个关键因素。这个问题已成为最近几年来国内外研究的一个热点,本书全面介绍了 Web 服务涉及的主要安全问题和可能采取的安全技术。

本书在简要介绍企业应用集成技术的发展现状的基础上,介绍了企业应用集成的中间件技术、Web 服务技术和栅格技术等,全面讲解了信息安全基本知识、面向服务的体系构架和 Web 服务技术、Web 服务关键协议及其安全性、Web 服务安全认证和访问控制机制、攻击建模方法、网格攻击体系和 Web 服务攻击技术,以及 NCES 的系统架构和核心服务,并对服务发现核心服务和安全核心服务所使用的关键技术进行了详细分析。

本书的内容中既有较深的理论研究,又有丰富的实用技术。全书结构合理,并且内容丰富,可供相关领域科研和工程技术人员参考,也可作为相关专业高年级本科生和研究生的教学参考书。

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。  
版权所有,侵权必究。

### 图书在版编目(CIP)数据

Web 服务安全 / 马恒太等编著. —北京: 电子工业出版社, 2007.12  
(安全技术大系)  
ISBN 978-7-121-04923-1

I. W… II. 马… III. 计算机网络—安全技术 IV. TP393.08

中国版本图书馆 CIP 数据核字(2007)第 132656 号

责任编辑: 葛 娜

印 刷: 北京市天竺颖华印刷厂

装 订: 三河市金马印装有限公司

出版发行: 电子工业出版社

北京市海淀区万寿路 173 信箱 邮编 100036

开 本: 787×980 1/16 印张: 31.5 字数: 597 千字

印 次: 2007 年 12 月第 1 次印刷

印 数: 4000 册 定价: 59.80 元

凡所购买电子工业出版社图书有缺损问题,请向购买书店调换。若书店售缺,请与本社发行部联系,联系及邮购电话:(010) 88254888。

质量投诉请发邮件至 zltz@phei.com.cn, 盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线:(010) 88258888。



# 安全技术大系



解析安全技术的各种核心问题，  
彰显领域专家的理论与实践水平，  
反映安全技术的最新应用，提供完整的解决方案！  
在相对专业、受众较窄的领域里，  
以我们的眼光和质量，  
**创造安全技术大系一个个畅销传奇！**

**投稿热线：**  
(010)88254013, 88254368  
**投稿邮箱：**bn@phei.com.cn

为了使您通过本书更透彻地了解信息安全行业发展动态，学习信息安全新技术，掌握信息安全实际技能，我们将特别为您提供一系列后续的服务，包括提供本书的修订和升级内容、本书作者的见面会，以及相关领域的会议、培训优惠。

您只要将下面序列号，移动用户发短信至62621666116，联通用户发短信至70226666116，或者发电子邮件至market@broadview.com.cn，具体相关信息我们将实时发短信与您联系。

序列号：

**04923**



# 企业网络与信息安全培训

在科学技术发展的今天,越来越多的企事业单位进行了信息化改革,计算机和计算机网络大大地改变了人们的工作和生活方式,尤其是Internet和Intranet的广泛使用为企业的管理、运营和统计等带来了前所未有的高效和快捷。但同时计算机网络的安全隐患亦日益突出,很多企事业单位发现不知如何保障自身资源与信息的安全性,例如花了十几万甚至上百万买来的安全设备却往往发现,放在那里无从管理,不能发挥应有的功能与效果;面对越来越多的病毒泛滥、黑客入侵事件却束手无策。

因此,大家慢慢形成一个共识:网络安全问题的解决,关键在于人。

一个安全的网络系统的保护不仅和系统管理员的系统安全知识有关,而且和领导的决策、工作环境中每个员工的安全操作等都有关系。

所以,电子工业出版社华信知识服务平台推出的“企业网络与信息安全”分为对员工的培训、对IT部门人员的培训、对主管IT的领导的培训,建立一个立体化的培训体系。全方位地解决企业的网络与信息安全问题。

## 一、课程内容

课程名称:企业网络与信息安全(2008年6月前每月一期)

课程小节	适合对象	课时
企业员工信息安全意识和技能培训	普通员工	1天,6学时
反黑客攻防技术 防火墙与网络隔离技术 漏洞扫描与入侵监测技术 拒绝服务攻击检测与防御 授权与身份认证技术 VPN技术 网络安全应急响应 无线网络安全	IT部门人员	5天,30学时
网络安全对企业的重要性 信息安全法规、政策 信息安全风险评估与管理 企业信息安全体系规划与建设	主管IT的领导	2天,12学时

## 二、开课时间及收费

请见www.sinoit.org.cn

# 网站安全保护培训

网站安全问题已成为目前政府、电子商务、企业信息化需要关注的主要问题。网站被攻击对于政府来说会损害政府形象;对于公司来说,不仅有损公司声誉,影响公司业务,而且不可避免将失掉很多潜在的顾客,如果再造成商业资料和顾客资料遭窃,那对电子商务将是致命的打击。

那么怎么才能防患于未然,在遇到黑客、病毒攻击后迅速响应,恢复网站的正常呢?

电子工业出版社华信知识服务平台鼎力推荐的“网站安全保护”培训课程,使您的问题迎刃而解。

## 一、课程内容

课程名称:网站安全保护(每月一期)

课程小节	内容
1. 操作系统安全	操作系统安全, IIS服务器安全, Apache安全
2. 网络安全	服务器、防火墙、入侵检测和路由器等的合理编配, 设置等。
3. 防DOS(拒绝服务攻击)	防拒绝服务攻击常用技术及解决方案
4. 数据库安全	SQL Server数据库安全技术, Oracle数据库安全技术
5. 网页防篡改及其恢复	防网页篡改常用技术及解决方案
6. 安全管理	补丁更新管理、日志管理、用户管理、日常管理制度, 应急响应等。

## 二、教学方式

- 专家教授讲授与案例式分析相结合的体验式教学方式。
- 通过研讨和讲座, 积极互动、深度沟通等形式, 解决学员的个案问题。

## 三、网上查询

培训时间、学费、报名方法等  
请到www.sinoit.org.cn网站查询。

主办单位: 电子工业出版社

咨询电话: 010-88254012 / 88254013

手机: 13911757806

联系人: 毕宁 E-mail: bn@phei.com.cn

网站: www.sinoit.org.cn



## 《Web 服务安全》读者交流区

尊敬的读者：

感谢您选择我们出版的图书，您的支持与信任是我们持续上升的动力。为了使您能通过本书更透彻地了解相关领域，更深入地学习相关技术，我们将特别为您提供一系列后续的服务，包括：

- 提供本书的修订和升级内容、相关配套资料；
- 本书作者的见面会信息或网络视频的沟通活动；
- 相关领域的培训优惠等。

请您抽出宝贵的时间将您的个人信息和需求反馈给我们，以便我们及时与您取得联系。

您可以任意选择以下三种方式与我们联系，我们都将记录和保存您的信息，并给您提供不定期的信息反馈。

### 1. 短信

您只需编写如下短信： 04923 +您的需求+您的建议

移动用户发短信至62621666116，联通用户发短信至7022666116。（资费按照相应电信运营商正常标准收取，无其他收费）

### 2. 电子邮件

您可以发邮件至 [jsj@phei.com.cn](mailto:jsj@phei.com.cn) 或 [editor@broadview.com.cn](mailto:editor@broadview.com.cn)。

### 3. 信件

您可以写信至如下地址：北京万寿路173信箱博文视点，邮编：100036。

如果您选择第2种或第3种方式，您还可以告诉我们更多有关您个人的情况，及您对本书的意见、评论等，内容可以包括：

- (1) 您的姓名、职业、您关注的领域、您的电话、E-mail地址或通信地址；
- (2) 您了解新书信息的途径、影响您购买图书的因素；
- (3) 您对本书的意见、您读过的同领域的图书、您还希望增加的图书、您希望参加的培训等。

同时，我们非常欢迎您为本书撰写书评，将您的切身感受变成文字与广大书友共享。我们将挑选特别优秀的作品转载在我们的网站（[www.broadview.com.cn](http://www.broadview.com.cn)）上，或推荐至CSDN.NET等专业网站上发表，被发表的书评的作者将获得价值50元的博文视点图书奖励。

我们期待您的消息！

博文视点愿与所有爱书的人一起，共同学习，共同进步！

通信地址：北京万寿路 173 信箱 博文视点（100036）

电话：010-51260888

E-mail：[jsj@phei.com.cn](mailto:jsj@phei.com.cn)，[editor@broadview.com.cn](mailto:editor@broadview.com.cn)



## 反侵权盗版声明

电子工业出版社依法对本作品享有专有出版权。任何未经权利人书面许可，复制、销售或通过信息网络传播本作品的行为；歪曲、篡改、剽窃本作品的行为，均违反《中华人民共和国著作权法》，其行为人应承担相应的民事责任和行政责任，构成犯罪的，将被依法追究刑事责任。

为了维护市场秩序，保护权利人的合法权益，我社将依法查处和打击侵权盗版的单位和个人。欢迎社会各界人士积极举报侵权盗版行为，本社将奖励举报有功人员，并保证举报人的信息不被泄露。

举报电话：(010) 88254396; (010) 88258888

传 真：(010) 88254397

E-mail: dbqq@phei.com.cn

通信地址：北京市万寿路 173 信箱

电子工业出版社总编办公室

邮 编：100036

# 序

Web 服务是面向对象和组件化的合理发展，它的出现激发了分布计算模式的转变，体系结构迅速从分布式对象体系结构（DOA）向面向服务的体系结构（SOA）转换。相比较而言，面向对象和组件化的方法在复杂的大型系统设计中经受住了考验，而 Web 服务则正在经受考验。Web 服务继承了面向对象的封装、消息传递、动态绑定、服务描述和查询等基本概念；基于 Web 服务的发布和订阅机制，用户可以方便地进行 API 的网络引用，并且不必考虑 API 的实现细节。但是，这一优点在实际应用中带来许多便利的同时，也面临安全问题的巨大挑战。目前，安全问题是制约 Web 服务发展的主要瓶颈，也是 Web 服务能否为大众所接受，能否得以迅速推广的关键。

Web 服务面临的安全挑战包括：原有系统的安全机制的影响和引用，以及针对服务发布、查找和引用过程的安全防护。《Web 服务安全》一书对这些安全问题产生的原因、机理和研究现状进行了详细讨论，对基于 Web 服务的系统应用集成提供了多种解决方案，可帮助系统规划者在集成设计过程中，充分考虑安全因素的影响。

Web 服务在企业应用集成方面有迫切的需求。特别是军事信息系统的发展，随着“以武器平台为中心”逐渐向“以网络为中心”的陆海空天一体化作战模式转变，Web 服务和栅格技术相结合，为军事信息系统集成提供了合理的实施思路，并已有成功的实例。例如，美军的全球信息栅格（GIG）就是基于 Web 服务技术的网络核心企业服务（NCES），可在各军兵种信息系统之间实现互操作，并为此定义了 9 种核心服务。《Web 服务安全》一书对此进行了详细的介绍，并对一些关键安全问题进行了总结和分析，为基于 Web 服务的应用集成提供了指导方向。

攻与防是一柄双刃剑。网络 Web 服务攻击体系是从攻击者角度来分析 Web 服务的安全问题，这些内容虽然是从攻击体系构建和攻击技术设计的角度来介绍，但从中可以更清晰地了解基于 Web 服务的集成系统的安全问题。



《Web 服务安全》一书全面地探讨了 web 服务的安全问题，内容新颖，弥补了这一领域书籍稀缺的遗憾，对从事企业信息系统开发和集成的工程技术人员，以及从事网络安全技术研究的科研人员都有所裨益。

诚然，Web 服务是一项正在发展中的新兴技术，本书的讨论和研究还仅仅是开始，期望作者在再版中不断引入新的观点与解决方案，以飨读者。

受本书作者马恒太和李鹏飞两位博士的盛情邀请，是为序。

卿斯汉

谨识于北京中国科学院软件研究所

2007 年 10 月

# 前 言

Web 服务是描述一些操作（利用标准化的 XML 消息传递机制可以通过网络访问这些操作）的接口。Web 服务是用标准的、规范的 XML 概念描述的，称为 Web 服务的服务描述。这一描述囊括了与服务交互需要的全部细节，包括消息格式（详细描述操作）、传输协议和位置。该接口隐藏了实现服务的细节，允许独立于实现服务基于的硬件或软件平台和编写服务所用的编程语言使用服务。这允许并支持基于 Web 服务的应用程序成为松散耦合、面向组件和跨技术实现。

Web 服务技术是最近几年迅速兴起的一种应用集成技术，而安全问题是影响该技术广泛应用的一个关键因素。这个问题已成为最近几年来国内外研究的一个热点。Web 服务的安全性问题主要涉及到两个方面：原有系统的安全机制的影响和引用，针对服务发布、查找和引用过程的安全防护。本书全面介绍了 Web 服务涉及的主要安全问题和可能采取的安全技术。

## 本书主要内容

---

全书共分 7 章，主要内容如下：

第 1 章：企业应用集成及集成技术，简要介绍了企业应用集成的实现技术及技术发展，以及中间件技术、Web 服务技术等企业应用集成关键技术。

第 2 章：安全基础知识，主要介绍了密码体制，以及基本安全属性、基本安全机制和分层安全保障机制。

第 3 章：面向服务的体系构架和 Web 服务，主要介绍了面向服务的体系结构、Web 服务技术、Web 服务体系结构以及 Web 服务的协议体系。

第 4 章：Web 服务关键协议的安全性，主要介绍了 Web 服务关键协议安全性分析、Web 服务安全应用协议脆弱性分析和协议安全性分析方法及工具等。

第 5 章：Web 服务安全认证和访问控制机制，主要介绍了基础支撑系统 XKMS、安全断言标识语言 SAML、Web 服务身份管理、访问控制框架、策略描述语言 XACML，以及 Web 服务访问控制实践。

第 6 章：网络 Web 服务攻击体系与技术，主要介绍了攻击建模基本概念、方法，网络攻击体系总体目标、设计原则及结构，以及 Web 服务攻击技术分析。

第 7 章：网络核心企业服务集成系统 NCES，主要介绍了 NCES 系统总体架构、服务发现核心企业服务体系架构和安全服务核心企业服务体系结构，以及 NCES 未来的工作。

## 本书主要特色

---

本书的内容中既有较深的理论研究，又有丰富的实用技术。全书结构合理，内容丰富，可供相关领域科研和工程技术人员参考，也可作为相关专业高年级本科生和研究生的教学参考书。

本书由马恒太、李鹏飞、颜学雄、洪志国编写，蒋建春、季庆光和邓勇等为本书的编写提供了帮助和支持，在此表示感谢！本书在编写过程中参考了很多文献及书籍，在此对这些文献及书籍的作者表示感谢！

书中疏漏与错误在所难免，敬请广大读者批评指正。

作者

2007 年 10 月

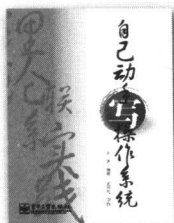
# 技术凝聚实力 专业创新出版

博文视点 (www.broadview.com.cn) 资讯有限公司是电子工业出版社、CSDN.NET、《程序员》杂志联合打造的专业出版平台, 博文视点致力于——IT专业图书出版, 为IT专业人士提供真正专业、经典的好书。

请访问 [www.dearbook.com.cn](http://www.dearbook.com.cn) (第二书店) 购买优惠价格的博文视点经典图书。

请访问 [www.broadview.com.cn](http://www.broadview.com.cn) (博文视点的服务平台) 了解更多更全面的出版信息; 您的投稿信息在这里将会得到迅速的反馈。

## 博文本版精品汇聚



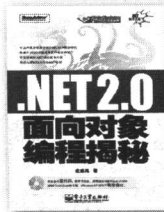
### 自己动手写操作系统

用理论指导动手实践, 用实践深化理解理论。

出版一年累计销量20000册, 广受读者好评!

于渊 编著 尤晋元 审校

ISBN 7-121-01577-3 48.00元 (含光盘1张)



### NET 2.0面向对象编程揭秘

从跨语言角度全面介绍C#2.0语言特性展示VS2005集成开发环境实用技巧系统剖析.NET核心技术内幕深入探讨CLR内部运行机理

金旭亮 著

ISBN 978-7-121-03975-1 69.8元 (含光盘1张)



### 游戏之旅——我的编程感悟

历时一载写就, 凝结十年心得。《仙剑奇侠传》之父姚壮宪热情推荐, 技术作家孟岩高度评价!

云风 著

ISBN 7-121-01609-5 46.00元



### SOA原理.方法.实践

IBM资深架构师——毛新生主编  
IBM中国开发中心技术经典呈现!

毛新生 主编

ISBN 978-7-121-04264-5 49.80元

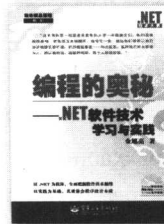


### Windows环境下32位汇编语言程序设计(第2版)

畅销书升级版!

罗云彬 编著

ISBN 7-121-02260-5 79.00元 (含光盘1张)

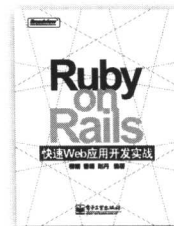


### 编程的奥秘——.NET软件技术学习与实践

步入编程之门, 领略软件之美! 以.NET为载体, 全面把握软件技术脉络! 以实践为基础, 直观体会程序设计本质!

金旭亮 著

ISBN 7-121-01820-9 65.00元 (含光盘1张)



### Ruby on Rails快速Web应用开发实战

国内第一本原创RoR图书。实例引导, 学以致用!

柳晴、曹璐、赵丹 编著

ISBN 7-121-02913-8 39.00元



### Ajax开发精要——概念、案例与框架

国内第一本重量级原创Ajax图书, 由一线开发人员编写, 上市以来持续热销!

柯自聪 编著

ISBN 7-121-02468-3 45.00元

博文视点资讯有限公司

电话: (010) 51260888 传真: (010) 51260888-802

E-mail: [market@broadview.com.cn](mailto:market@broadview.com.cn) (市场)

[editor@broadview.com.cn](mailto:editor@broadview.com.cn) [jsj@phei.com.cn](mailto:jsj@phei.com.cn) (投稿)

通信地址: 北京市万寿路173信箱 北京博文视点资讯有限公司

邮编: 100036

电子工业出版社发行部

发行部: (010) 88254055

门市部: (010) 68279077 68211478

传真: (010) 88254050 88254060

通信地址: 北京市万寿路173信箱

邮编: 100036

博文视点·IT出版旗舰品牌

# 目 录

第 1 章 企业应用集成及集成技术 .....	1	2.3 基本安全机制 .....	51
1.1 大型系统应用集成是时代的要求 .....	1	2.3.1 认证机制 .....	52
1.1.1 社会经济和商业发展的需求 .....	1	2.3.2 授权和访问控制 .....	63
1.1.2 未来信息化战争的需求 .....	4	2.3.3 加密和签名机制 .....	72
1.1.3 互连、互通、互操作能力是 大型应用集成的基础 .....	7	2.4 分层安全保障机制 .....	81
1.2 企业应用集成 .....	9	2.4.1 OSI 安全体系结构模型 .....	82
1.2.1 企业应用集成技术的发展 .....	9	2.4.2 网络层安全保障 .....	86
1.2.2 企业应用集成的实现技术 .....	12	2.4.3 传输层安全保障 .....	88
1.3 企业应用集成关键技术 .....	17	2.4.4 应用层安全保障 .....	91
1.3.1 中间件技术 .....	17	参考文献 .....	93
1.3.2 Web 服务技术 .....	19	第 3 章 面向服务的体系构架和 Web 服务 .....	94
1.3.3 网格技术 .....	23	3.1 面向服务的体系结构 .....	94
1.3.4 Web 服务与网格技术的 结合 .....	30	3.2 Web 服务技术 .....	97
参考文献 .....	31	3.2.1 Web 服务描述 .....	99
第 2 章 安全基础知识 .....	34	3.2.2 服务发现 .....	101
2.1 密码体制 .....	34	3.2.3 服务交互 .....	108
2.1.1 对称加密体制 .....	34	3.2.4 服务合成 .....	109
2.1.2 公开密码体制 .....	41	3.3 Web 服务体系结构 .....	110
2.2 基本安全属性 .....	44	3.3.1 总体结构 .....	110
2.2.1 机密性 .....	44	3.3.2 Web 服务的内部结构 .....	111
2.2.2 完整性 .....	45	3.3.3 Web 服务的外部结构 .....	113
2.2.3 非否认性 .....	46	3.4 Web 服务的协议体系 .....	115
2.2.4 可用性 .....	48	3.4.1 Web 服务协议集 .....	115
		3.4.2 Web 服务安全协议 .....	142
		参考文献 .....	158

第4章 Web 服务关键协议的安全性	161	5.5.2 XACML 上下文	299
4.1 Web 服务关键协议安全性分析	162	5.5.3 安全和隐私方面的考虑	302
4.1.1 XML 安全性协议分析	162	5.6 Web 服务访问控制实践	305
4.1.2 SOAP 安全性协议分析	180	5.6.1 Web 服务身份验证	305
4.2 Web 服务安全应用协议脆弱性分析	189	5.6.2 应用 XACML 实现访问控制的实例	312
4.2.1 基于 WS-Security 的认证协议脆弱性分析	189	参考文献	320
4.2.2 基于 SAML 的 SSO 协议脆弱性分析	203	第6章 网格 Web 服务攻击体系与技术	322
4.3 协议安全性分析方法及工具	215	6.1 攻击建模基本概念	324
4.3.1 协议安全性分析方法	215	6.1.1 攻击建模的目标和作用	324
4.3.2 典型分析工具——FDR 和 CASPER	223	6.1.2 主要术语和概念	325
参考文献	224	6.2 攻击建模方法	327
第5章 Web 服务安全认证和访问控制机制	226	6.2.1 基本原则	327
5.1 基础支撑系统——XKMS	227	6.2.2 攻击建模过程	328
5.1.1 PKI 和 XKMS 的关系	227	6.3 网格攻击体系	358
5.1.2 XKMS 协议	230	6.3.1 网格攻击体系总体目标	358
5.2 安全断言标识语言——SAML	260	6.3.2 网格攻击体系设计原则	359
5.2.1 跨域访问	260	6.3.3 网格攻击体系结构	360
5.2.2 SAML 概述	263	6.4 Web 服务攻击技术	365
5.2.3 SAML 断言	264	6.4.1 Web 服务攻击技术分类	365
5.2.4 SAML 协议	269	6.4.2 信息收集及分析技术	368
5.3 Web 服务身份管理	271	6.4.3 Web 服务攻击技术	388
5.3.1 .NET Passport	272	6.4.4 针对 Web 服务支撑环境的攻击技术	406
5.3.2 自由联盟工程	276	6.4.5 针对 Web 服务虚拟机的攻击技术	412
5.4 访问控制框架	280	参考文献	420
5.4.1 基本概念	280	第7章 网络核心企业服务集成系统 NCES	422
5.4.2 访问控制框架	281	7.1 NCES 系统总体架构	422
5.5 策略描述语言——XACML	282	7.1.1 未来网络中心战结构	423
5.5.1 XACML 策略语言模型	283		

7.1.2 NCES 体系结构.....	425	7.2.2 安全服务核心企业服务 体系结构.....	452
7.2 NCES 系统分解.....	427	7.3 NCES 未来的工作.....	488
7.2.1 服务发现核心企业服务 体系架构.....	427	参考文献.....	490

# 第 1 章 企业应用集成及集成技术

## 1.1 大型系统应用集成是时代的要求

### 1.1.1 社会经济和商业发展的需求

在 20 世纪的六七十年代，计算机开始用于民间企业。应用的主要目标是利用计算机来代替一部分联系不那么密切、手工且重复性的工作环节，以提高生产效率。这一阶段还没有企业数据或应用的集成需求。

到了 20 世纪 80 年代，全球企业在信息系统上进行了巨大投资，建立了众多的应用信息系统，以帮助企业处理和管理内部或外部业务。由于企业的传统结构是按照职能来组织各个部门，各个部门分别担负相关的职能，也分别使用不同的应用信息系统来协助它们完成规定的职能。从而导致众多关键的信息被封闭在相互独立的系统中，形成一个所谓的“信息孤岛”。如何将众多的“信息孤岛”联系起来，以便让不同的系统之间交互信息，作为一个企业需求被提出来。由此，系统应用集成的价值和必要性也开始体现，企业在追求效率和控制成本，或在兼并和收购过程中，对应用集成技术提出了更高的要求。特别是电子商务的兴起，这一基于 Internet 的新商务模式直接导致了 Web 服务技术的出现。这时企业应用集成（EAI）不仅仅是企业面临的一个技术问题，还是一个管理问题和组织问题。

大型企事业单位在多年持续不断的信息化建设过程中，先后引入不同时期的技术和软、硬件平台，并陆续建立了许多应用系统。正是由于这些历史原因，当前企业级信息集成通常要面对各种各样的硬件平台、操作系统、编程语言、软件技术、数据管理系统，



以及各种具体业务应用。企业级应用系统需要进行复杂的业务处理并解决复杂的协调问题，其本身早已从单一的数据库应用系统演变成了一个网络环境下由人员、设备和信息组成的分布和异构的复合系统。随着需求的变化和技术的发展，企业级应用系统逐渐从以纵向业务为中心的孤立式应用，朝着面向企业内外的业务流程和动态协同工作的集成化信息系统的过渡，以提高企业整体上的协同能力、快速反应能力、适应能力和电子商务能力。

围绕现代企业级应用系统构筑的问题，应用集成的方法、技术和工具近来又一次成为信息技术领域备受关注的焦点。人们在实践中逐渐认识到，企业级应用集成不是一件一劳永逸的事情，而是一个持续的过程。在现代社会环境中，各企事业单位都要面对快速变化的运作环境和社会需求，尤其是近年来网络计算环境的发展促进了经济全球化。在 Internet 经济时代，企业无法在完全独立的“真空”环境下运营，迟早要卷入到电子商务的大潮之中。这些都要求企业的信息系统必须能够依据新的需求，快速且灵活地集成各种已有的和新添置的业务应用系统，并使得它们即时、有机地协同起来为企业的业务活动提供服务。无论是从企业内部信息化发展的角度，还是从实施基于 Internet 的电子商务的角度考虑，柔性化信息系统基础设施的建设，以及支持应用集成和协同工作的技术和工具都是核心问题。

(1) 传统应用集成主要包括了界面集成、数据集成和过程集成 3 个层次。其中，界面集成是最浅层次的，只是把原有零散的系统界面集中在一个新的，通常是浏览器的界面中；数据集成是为新的商业目的提供一个可访问已有多个数据库系统的新接口，即使数据集成也是不够的，因为数据的意义还体现在数据之外的约束和处理上；过程集成是最高层次的集成，只有它才能最好地实现新的商务目标。商业过程的集成通常也称为“业务集成”(Business Integration)，B2Bi (Business to Business Intergration) 就是这样的一种“过程集成”或“业务集成”。业务集成的实现手段通常是采用传统的中间件或 EAI 技术，主要包括基于消息中间件、交易中间件或者应用服务器的集成。基于专门的“消息中介”的业务集成具有的共同特点是集成一般是紧耦合的，整体的处理效率很高。但集成基于各中间件或集成平台产品专有 API，或某种对象模型，需要以专有 API 或按照特定对象模型规范编写新的模块，并有较深的学习曲线，对业务变化的适应性差，具有一定的局限性。

(2) 基于 SOA (面向服务架构) 和 Web 服务技术的应用集成是业务集成技术上的一次重要变化，集成的对象是一个个的 Web 服务或者是封装成 Web 服务的业务处理。Web 服务技术由于基于广为接受且开放的技术标准，如 HTTP、SMTP、SOAP (Simple Object Access Protocol, 简单对象访问协议)、WSDL (Web Service Description Language, Web 服务描述语言) 和 UDDI (Universal Description Discovery and Integration, 通用描