某电子商务系统的解决方案

1 项目需求

1.1 功能需求

xxx 电子商务系统主要功能分为前台功能、后台管理功能和资讯管理功能。其前台功能主要是商品购买模块及会员信息模块，实际上还应包括网站首页，资讯浏览模块等。其后台管理功能主要分为基础信息管理、销售业务管理、用户管理、财务管理、数据统计分析和系统功能。其资讯管理功能主要是新闻发布管理、商品信息管理和商品资讯管理等。

1.2 性能需求

根据业务需求，本系统的用户主要是互联网网民。这些用户可以分为两类，第一类是会员，即已经注册可购买商品的网民，第二类是游客，即还没有注册的浏览者。游客主要访问网站首页和资讯页面，了解网站功能，了解商品信息等。会员的主要操作是商品购买和售后服务，即使用网上购物模块。

参考典型电子商务网站的统计数据，其日均页面访问量为 100 万以上，其中 35%为首页和资讯页面的访问。首页和资讯页面可采用静态网页方式发布，提升访问速度和处理性能。统计数据表明，访问量中约 35%是商品购买操作相关的。这部分访问的是动态网页，需要操作数据库。按照日均 100 万页面访问量计算，约 35 万动态页面访问量。

作为大型互联网服务网站，要求具有 365*7*24 小时的稳定运行能力。最好具有负载均衡、故障屏蔽和抗毁容灾能力，且系统没有单一故障点。

网站涉及电子交易、出票等和经济相关的操作。系统一旦被攻破，将带来很大的经济损失，因此需要考虑整个系统的安全性。

2 系统设计

2.1 部署结构

本解决方案采用数字有机体系统作为服务主体，结合安全和可靠性需求，建议的部署结构如图 1 所示。

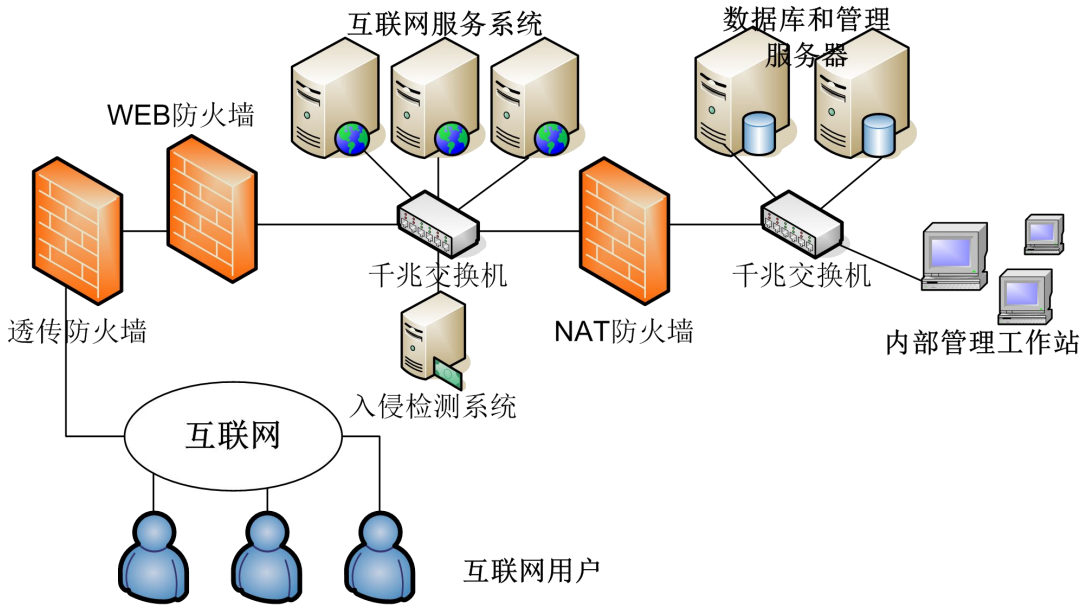

图 1 系统部署结构图

从安全性考虑，该解决方案采用异构防火墙建立两个不同安全等级的区域。第一个防火墙后的区域用于提供互联网服务，并不保存敏感数据。第二个防火墙采用第一个防火墙的异构防火墙（不同厂家不同类型的防火墙），建立一个更加安全的区域，用于保存业务数据和提供内部管理服务。

为进一步提高系统的安全性，建议部署 WEB 防火墙来提供针对性的 WEB 服务保护。部署入侵防御系统来检测入侵，并及时调整防火墙策略，提升系统安全性能。

互联网服务系统采用数字有机体系统。它将多台服务器整合为一个系统，实现大规模网络服务，提供诸如负载均衡、故障屏蔽、虚拟服务器、共享文件系统等服务，从而使得系统性能可以通过增加服务器来近似线性的扩展。数据库和管理服务器也采用数字有机体系统，提高数据可用性和查询性能等。

内部管理人员在企业网内通过网络访问管理服务器来进行系统管理工作，如

发布资讯，统计财务等。

2.2 软件结构

本解决方案的业务系统采用如图 2 所示的软件结构。

图 2: 软件系统结构

系统层采用数字有机体系统，包含提供数据库服务的数字有机体工作库，提供文件服务、负载均衡、虚拟服务等的数字有机体工作平台，以及提供大规模数据存储，抗毁容灾的系统组件。

应用支撑层面的基础是 J2EE 平台。他是当前最流行的大型网站系统基础平台，能够适应不同应用环境和应用规模。Web 服务采用 Apache 配合 JBOSS 方式。Apache 能够充分利用具有多路 CPU 的高性能服务器的处理能力，并且在高并发下具有稳定的性能。JBOSS 适合具有复杂业务逻辑的 WEB 业务服务，能够提供广泛的应用支撑，是理想的动态网站支撑平台。将 Apache 和 JBoss 配合，由 Apache 提供静态页面服务，由 JBoss 实现复杂业务逻辑。同时，利用 Apache 的 Web 集群功能，还可实现单机内多个 JBoss 实例的负载均衡，从而进一步挖掘高性能服务器的处理能力。

应用业务的实现采用 Struts+Spring+Hibernate 集成框架。其他的业务实现技术，如 ESB，XML、消息队列、数据持久化等，在网站建设中已经普遍采用。

各个业务模块可以根据业务逻辑进行划分，分别实现不同的业务功能。

3 安全设计

系统安全需要从多方面保证，这包括网络安全、系统安全、数据库安全、服务程序安全和应用程序安全。

3.1 网络安全

从安全性考虑，系统采用双异构防火墙结构，并建议采用不同厂家的产品。本系统只有 WEB 服务，为了进一步增强系统的安全性，建议部署一台 WEB 防火墙。如果还需要进一步增强系统的安全性，可以考虑再部署一套入侵防御系统。

3.2 系统安全

服务系统采用数字有机体系统。为提升操作系统安全，将对操作系统进行以下加固。

1）启用强制访问控制机制，严格限制每个程序的访问范围，提升系统安全。

2）启用数字有机体主机防火墙，为系统提供抵抗网络攻击的能力。

3）启用加密通信和主机认证机制，保证数据传输的安全。

4）用户账号安全加固：对系统密码安全策略、密码安全性、密码文件访问等进行加固，抵御密码暴力破解、密码文件篡改、长期使用密码泄露等问题。

5）防 DDOS 攻击：启用反 DDOS 攻击，限制每个 IP 每秒的连接量。

6）其他安全加固：如敏感文件访问限制，资源使用限制，日志系统安全设置等，以杜绝其他漏洞。

3.3 数据库安全

1）从安全存储考虑，建议将数据库系统部署在内部安全区域。

2）在数据库上，对敏感数据，如用户口令等，采用加密存储。

3）在数据库系统上配置访问控制，只允许指定服务器访问数据库，从而防

止外部非法访问。

4）设置合理的访问权限，将管理、应用服务和运行维护人员的权限分开，分别授予不同权限。最小化各个用户的访问权限。

3.4 服务程序安全

本系统主要采用的服务程序是 JDK、APACHE、JBOSS、Struts、Spring 和 Hibernate 等。这些服务程序本身也存在一些漏洞，从而为攻击者提供了方便。为此，需要将上述软件更新到可靠的版本，并打上已经发现的各种安全补丁。

但是，安全漏洞在不断地发现。如果长时间不打补丁，也可能为攻击者留下机会。因此，一方面需要安全管理员经常关注各个服务软件的新安全漏洞，并及时打上补丁。另一方面可以采用 WEB 防火墙，在防火墙上开启软件的虚拟补丁功能，从而在安全管理员未及时打补丁的情况下抵御攻击。

3.5 应用程序安全

应用程序本身的实现也要考虑安全性。本解决方案主要采用的技术如下。

1）静态页面发布：对于访问量大且数据更新周期不是很短的页面可以采用动态页面静态化。

2）密码存储：如限制密码的长度，检测输入的密码是否为键盘字符，通过变换不同的算法来增加密码的长度等。

3）会员身份认证：对于 VIP 会员，发放存有数字证书的 USBKEY。

4）会员交易数字签名：对于 VIP 会员的交易，用 USBKEY 内的私钥对摘要信息进行加密即数字签名。

5）交易请求加密传输：所有的交易过程都采用 SSL 加密机制。

6）防 SQL 注入。

7）防 XSS 攻击。

4 性能设计

4.1 优化系统性能

本解决方案将从三个层面优化系统性能。在系统层面，通过数字有机体系统实现多机负载均衡，提升系统服务能力。在数据库层面，通过表分片技术、读写分离等，利用数字有机体系统提升数据库性能。在应用层面，通过静态页面化、WEB 缓存技术等提升应用服务性能。整合三个层面，从而为系统性能扩充提供无限支持。

4.1.1 系统层面

本解决方案采用数字有机体系统作为服务平台。数字有机体系统不仅对单机性能进行了全面优化，还提供全局负载均衡和虚拟服务器等功能，使 WEB 应用性能得到提升，并具有在线扩展能力。

1）多机协同服务

数字有机体系统不仅对单机性能进行优化，还提供多机和多区域协同服务能力。这种能力使得系统可以无限制的扩展，满足不短扩张的应用需求。

和常见的集群方案相比。数字有机体系统不需要单独购买硬件的负载均衡器，系统本身即可完成多达 16 台服务器的负载均衡，从而减少了硬件投资。从电信测试结果来看，系统性能整合的能力达到 80%以上。可以满足每秒上万事务处理的需求。这是大型网站常见的峰值需求。

同时，数字有机体系统提供全局一致的共享文件系统。这使得多台服务器间可以实时同步业务数据，并获得完全相同的文件访问支持。通常，这样的功能需要专业的集群文件系统和共享存储设备，如 SAN 的支持。这些软件和硬件需要大笔的费用投入。因此数字有机体系统减少了对共享存储设备（通常是 SAN）和集群文件系统的投入。

数字有机体系统提供虚拟服务器功能。多达 16 台服务器的系统可以只用单个公网 IP 进行访问，从而获得单一的互联网入口。该功能通常需要硬件负载均衡器才能实现。

数字有机体系统还提供在线扩展能力。该能力使得可以在不暂停系统运行的情况下，增加新的服务器来提升系统的服务能力。

3）多区域服务

数字有机体系统还提供多区域服务能力。该服务能力无需硬件存储设备来实现异地数据复制，也不需要人工复制数据，即可保证多区域使用相同的数据提供服务。同时，数字有机体系统提供多区域服务需要的就近服务调度和负载均衡能力。而这些能力只在某些大型数据中心的解决方案中才有。

4.1.2 数据库层面

在数据库层面，该解决方案可通过三种手段提升系统整体性能。

1）分库分表优化。

如果一个数据库过大，则需要一台服务器具有很大的内存和处理能力，而且对于大数据表的查询、修改都很慢。即使是 Oracle 数据库也需要采用分区或者分表的方式来实现。数字有机体数据库系统支持大量的数据库，并且支持对多个数据库并行进行操作，因此可以采用分库的方式提升系统服务能力。

对数据量较大的统计采用中间表的方式加快统计速度。例如将一天的交易统计转换为一条统计记录保存在单独的表中，这样即可加快每周和每月的统计效率。

2）数字有机体查询支持

数字有机体工作库支持将一个数据量很大的表分片存储。表的分片分别存储在不同的服务器上，由数字有机体工作库自动将查询任务分解到多台服务器上协同执行，从而可以利用多台服务器的处理能力来提升大数据查询的速度。这为系统提供了良好的大数据分析支持。

2）读写分离优化。

数字有机体数据库系统同时支持同步数据更新方式和异地更新方式。对关键的数据，例如会员基本信息和财务信息，可以单独建库，采用同步更新方式，确保多机数据一致。对其他数据，例如交易记录，登陆日志等。这些数据在一次写入后会频繁查询，可采用异步更新方式，获得更高的读写性能。通过读写分离后，单数据库的插入速度可以达到每秒上万次插入操作，而查询速度可随服务器数量

近似线性的增加。因此，这完全可以满足大型网站的应用需求。

3）多中心服务优化。

如果系统的规模进一步扩展，例如达到新浪和百度这样的规模，单个数据中心就无法提供服务了。在多数据中心情况下，需要实现多数据中心间数据的同步和异步复制。数字有机体系统同时提供文件系统和数据库系统的多中心数据复制和整合能力，使得应用可以像单中心系统一样进行开发和部署，从而简化系统开发难度。

在多中心服务模式下，用户就近获得服务，提升了服务质量。同时，网络流量分散到多个数据中心，减轻了获得大带宽的压力。另外，多个数据中心并行服务也提升了系统的容灾能力。即使某个数据中心奔溃，系统也仍然可以继续提供服务。

4.2 系统性能扩展

本解决方案具有良好的系统扩展能力。系统可以通过以下手段进一步扩展性能，几乎没有扩展限制。

1）服务器性能提升。这是传统的方式，包括增加服务器内存、增加处理器、增加内置硬盘、增加外接存储设备等。本方案的优势是系统采用多机并行服务，因此提升单机性能时无需停止服务。只需关闭要升级的服务器进行升级即可，其他服务器可以继续提供服务。

2）增加服务器。在一个数据中心（或者服务点），可以通过增加服务器的方式在线提升性能。增加服务器时，只需安装好数字有机体系统和服务软件，启动后服务器自动加入系统提供服务，从而在线提升系统服务能力。采用虚拟服务器时，单虚拟服务器最多支持 16 台服务器。通过分解业务系统为多个虚拟服务器的方式可进一步提升支持的服务器数。

3）增加服务中心。如果单服务中心因出口带宽限制无法提升性能时，还可以部署多服务中心来提升性能。数字有机体系统自动整合多个数据中心，实现数据中心间的数据同步、负载均衡、故障屏蔽和透明化服务等，从而高效的提升系统性能。

多服务中心不仅可以提升服务能力，而且在中国这种条块化网络下，更有利

于就近为网民提供服务，提升服务质量。传统的解决方案是 CDN，但它需要大笔的投入。

5 可靠性设计

本解决方案具有高可靠性的特点。它可从三个层面解决可靠性问题。

5.1 数据可靠性

本解决方案采用数字有机体系统存储文件数据和数据库数据。无论是文件还是数据库数据，系统都可以为其建立多个副本。这些副本可以分布在单个数据中心的多台服务器的存储系统中，也可以同时分布于多个数据中心的服务器的存储系统中。当在单数据中心分布时，相当于实现了多存储设备本地热备份。当在多个数据中心分布时，则相当于实现了异地热备份，从而可以抵御区域性灾难。

当任意一个副本因服务器故障、存储设备故障或者网络故障等无法访问时，系统自动为其增加副本，从而保证数据的可用性。并且业务程序可以继续访问数据，不会出现访问中断，从而进一步提升了数据可用性。这些功能都是普通解决方案没有的。

5.2 业务可靠性

本解决方案支持多机多数据中心协同服务，并且具有负载均衡、故障屏蔽和服务自动调度等功能，从而确保业务不停顿。

当在单数据中心采用多服务器协同服务时，也优于常见的集群方案。首先，系统每台服务器都可完成负载均衡，因此不需要集中的硬件负载均衡器。这就不会在硬件负载均衡器上形成单一故障点或者性能瓶颈。其次，服务的响应无需经过集中的节点返回，每台服务器可以独立的响应客户，从而提升了服务性能，并降低了系统故障概率。

当采用多数据中心部署模式时，各个数据中心之间可以形成异地热备份。系统自动实现数据中心间的就近调度，负载均衡和故障屏蔽。系统不会因为任何数据中心的故障，例如常见的网络故障、区域性停电等而停止服务。这进一步提升

了系统的可靠性。

5.3 系统可靠性

整个系统的可靠性不是由单一方面的技术就能解决的。例如 Oracle 的 RAC 只能解决小范围的数据库可靠性问题，而且存储设备故障时数据库服务即停止，无法解决文件数据可靠性，更不要说业务服务可靠性。对大规模的灾难来说，常见的集群方案也无法解决。而数字有机体系统同时整合数据可靠性、业务可靠性和系统部署等方面的解决技术，形成完成完整的系统的可靠性解决方案。

6 方案优点和特点

本解决方案的优点和特点如下：

1）高扩展性

如前所述，本解决方案性能扩展可以通过提升单机能力、增加服务器和增加服务中心的方式实现。整个系统的服务能力没有上限。

同时，本解决方案支持在线扩展。可以在不停止服务的情况下，提升服务性能，或者增加服务器数量等。从而消除常见的因系统升级而停止服务的情况。

2）高可靠性

系统同时解决了数据和业务的容灾抗毁。整个系统不存在单一故障点。

3）多层安全保障

本解决方案从网络层面、系统层面、数据库层面、服务程序层面和应用层面分别解决面临的安全问题，从而形成完整的多层安全防护体系，尽量消除可能存在的安全漏洞。

4）统一运维管理

本系统有数字有机体系统作为基础平台，利用数字有机体综合管理系统，可以实现对网络系统、安全设备、服务器、业务系统等的全面监控和管理，从而保证系统能够长期平稳运行。

5）高性价比

本解决方案无需购买昂贵的负载均衡器、SAN 存储设备、Oracle 数据库等，

采用常见的服务器构建服务系统，从而降低硬件和软件投入成本。

7 客户价值

1）利用高性价比的通用服务器构建高可靠，高安全的互联网服务平台，投资效益高。

2）可边收益边投入，无需冒一次性大投入的风险。系统具有良好的扩展性，可以根据需要增加服务器和服务站点，扩展系统规模，无需一次性建立整个系统。

3)系统具有良好的可靠性，能够自动处理各种故障，极大降低业务中断的风险。管理人员只需及时修复故障设备即可让系统不间断的运行。

4) 全面安全保障，系统安全无忧。解决方案从网络层面、系统层面、数据库层面、服务程序层面和应用层面分别解决面临的安全问题，从而形成完整的多层安全防护体系，尽量消除可能存在的安全漏洞。