信息网站的用户管理与实现

李森林 （安徽省财税信息计算中心 230061）

摘要：本文就Web信息网站用户管理的意义和主要内容进行了讨论，并介绍了用ASP技术实现信息网站用户管理的方法。

关键词：Intranet Web IP地址 ASP

1 管理策略

建在Intranet上的信息网站的服务对象均为内部人员，这就明确了内部信息网站用户管理的具体对象。内部信息网用户管理可分为基于操作系统型的和独立于操作系统型的。前者是对登录了网络的用户进行管理，可以依托网络操作系统提供的管理功能实施用户管理；而后者则不要求用户必须登录网络。比较而言，独立于网络操作系统型的用户管理具有更大的灵活性，可以大大简少系统管理的工作量，便于实现和实施远程管理。

由于内部网站和外部网站在辨识用户的方法和过程上大同小异，为简单起见，下面的讨论主要针对内部网站和内部人员。

2 用户管理的主要内容

用户管理工作通常包括系统IP地址分配、用户资料库管理、用户注册、用户级别设置、用户权限设置、用户日志和系统工作状态监控等主要内容。

2.1 IP地址分配管理

在Intranet建设规划时，有两种客户机IP地址分配策略。一种是静态IP地址分配策略，即由系统管理人员为每台客户机分配一个IP地址，并逐台将机器设置为指定的IP，从而很容易用对照表来反映用户与IP地址的对应关系。另一种是采用动态IP地址分配策略，即将客户机设置为自动获取IP地址状态，由系统的DHCP服务器自动为每台登录上网的客户机动态分配一个空闲的IP地址，在客户机离线前和预设的时间范围内，该IP地址对应于该客户机；而当该客户机在预设时间范围之外重新登录时，则会被系统的DHCP服务器重新分配一个空闲的IP地址。当预设的时间足够长时，动态IP地址和静态IP地址的使用效果是一样的，区别仅在于：客户机动态获得的IP地址在机器上不是显式设置的。系统经过一段时间的运行，也可以逐步建立起相对固定的用户IP地址对照表。

笔者认为，在IP地址资源不紧张的前提下，应尽可能采用静态IP地址分配策略，从而在IP地址和客户机及用户间建立起固定对应的关系，有助于系统管理。而静态IP地址分配工作比较繁琐的问题，可以采取借助IP地址注册统计程序来进行辅助处理（由程序自动搜索用户注册资料库，找出空闲的IP地址供用户选用），从而减小IP地址分配与管理的工作量。

2.2 用户资料库

顾名思义，用户资料库是为保存用户的基本人事资料（如姓名、性别、籍贯、出生日期、所在部门、职务等）而设置的，其目的是强制用户进行实名注册、核查用户注册时输入的个人资料是否正确。当用户首次登录网站，进行用户注册时，只有输入的个人资料与资料库保存的内容相一致时，才能完成整个注册过程，否则不能成功注册。

2.3 用户注册

用户注册是对网站用户进行分类、分级管理，保证系统有序运行的基础，用户注册信息是系统判别来访用户是否为注册用户的依据。在Intranet中，为保证系统安全和信息来源的可追溯，应采用实名注册机制，即在用户注册环节，采取将用户提交的个人资料与用户资料库信息进行比对的方法来进行判别与限制。因此，当新用户（IP）登录时，应由系统引导其进行注册，注册时，用户按照系统提示输入姓名、密码等个人信息。用户注册成功后，系统将用户个人信息与自动获取的客户机信息（如IP地址等）合成用户注册信息，保存到用户注册库中。用户注册资料是判别登录用户是否为注册用户的依据。

为防止别有用心的员工冒名注册，应将客户机IP地址、用户名、用户密码及其他个人信息进行捆绑验证。如

有必要，还可辅之以验证客户机MAC地址、限制用户注册次数等措施来保证用户注册环节的安全与可信。

2.4 用户登录

当客户机登录信息网站时，网站系统可以自动获取来访客户机的IP地址，并将该IP地址与用户注册资料库中的记录进行比对，以判别来访者是否为注册用户。其流程是：若在资料库中未找到该客户机IP地址相关的资料，表明是未进行过注册的客户机，则引导其进行用户注册。若用户注册库中存在该IP地址注册资料，表明该客户机已进行过注册，将提示用户输入其个人资料（姓名、密码等），然后再与用户注册库中的记录进行比对，验证用户密码、确认用户身份。

经确认的用户，将被系统自动赋予一个标识该用户且在客户机上不能获取和更改的、存活期可由系统控制的身份信息（如后述的session变量）。在系统设定的身份信息有效期内，该状态信息将伴随着用户的一切网上活动，用户在该身份信息的暗中伴随和约束下，可以进行系统允许的信息浏览和发布活动，并免除了在浏览操作过程中被系统反复提示输入密码的烦恼。用户身份信息也是网站系统准确统计信息资源利用情况的客观依据。

2.5 用户级别设置

Intranet用户在单位和组织机构内通常都有一个明确固定的工作岗位，属于某一部门和群组，位于某一行政级别（如处级/科级/办事员、部门经理/业务经理/业务员等），并享有该级别允许的网上活动（浏览、发布某类信息）。用户级别是确定用户浏览、发布权限的必要条件。用户级别由系统管理员根据人事资料和用户注册信息进行设置。上述的用户身份信息从属于用户级别的设置与管理。

2.6 用户权限设置

用户在网站上从事的主要活动是信息浏览和信息发布，为防止用户进行越权访问和随意性的信息发布活动，必须对用户进行权限限制。用户权限可分为阅览权和发布权，阅览权指是否允许用户阅览某类信息或某条信息。发布权指是否允许用户发布或更新某类信息。用户身份信息也从属于用户权限的设置与管理。

2.7 用户日志

用户日志是记录用户活动、统计信息栏目点击率、分析改进网络利用情况的第一手资料，用户日志保存到数据库中，便于日后的统计分析。利用用户日志信息能对诸如用户登录时间、浏览的站点与栏目、发布的信息等进行统计分析。

3 用户权限管理需求

上述用户管理的各个环节是环环相扣的关系，并最终体现在用户阅览权限和发布权限的设置与控制上。

在信息网站上，信息的存取是动态的、可交互式的过程。这种操作模式为发挥用户的主观能动性提供了便利条件，用户不单可以利用网上“搜索”功能来查找信息，还可以将信息直接在网站上发布，供本部门人员、指定的人员或全体网络用户共享，从而使用户身兼信息消费者和信息提供者的双重身份，在浏览信息的同时，又丰富和更新了网上信息，因此大大增强了信息网络的生命力。

出于信息安全的需要，对于网上的信息浏览和信息发布活动应加以必要的规范与限制，对在网上发布的信息进行分类和分级控制，根据信息的共享范围进行浏览限制。如只允许用户浏览公共信息和本部门、本群组的共享信息、允许某些用户浏览某类特定的信息（如财务主管可以浏览财务部的业务信息）、限制用户所能发布信息的种类等。

用户的行政级别与发布权限基本决定了用户的阅览权和发布权。但是，当某类或某条信息不能简单地以用户的群组和级别来划分阅览范围时，可以用户名的集合来设定阅览权限，在发布信息时指定阅览人员的姓名。当用户欲阅览该条信息时，其身份信息（姓名）若在指定阅览人员名单内，即可阅览该条信息。对于使用数据库而非静态网页形式存储和发布信息的系统而言，满足此类需求并非难事。

发布权限控制指限制用户可以发布信息的类别、要求发布人提供其姓名和密码并进行查验。应将发布人信息与其发布的信息一并存放到信息库中保存，既便于实时统计信息发布情况，又便于追查信息的发布责任。

4 用户管理的技术实现

4.1 工作环境

由于Web信息网站系统所依赖的HTTP协议是一种“缺少状态”的协议，导致客户机与服务器之间的每一个连接过程都是相互独立的，也没有执行Web常规任务的标准化方法。因此，在相当一部分网站系统中，Web页面之间不存在状态联系，服务器既不能记录客户机已经进行的访问过程，也不能记录访问过程中的各种参数。系统管理者要实现系统安全控制和用户权限管理时，只能采取诸如在网络操作系统中设置用户权限或封闭式网络运行等措施，不仅加大了系统管理的工作量，而且具有很大的局限性。

ASP (Active Server Page)技术非常适合于创建动态交互式的、具有多层体系结构的Web应用系统。ASP技术是在静态页面HTML内加入了可执行的SCRIPT语句，从而将HTML与可执行程序融合在一起，形成ASP页面文件，使Web页可以携带状态信息。当浏览器向服务器提出ASP页面文件请求时，Web服务器对该页进行解释并在服务器端执行，从数据库中自动提取用户所需的信息，并将动态生成的网页送至客户端的浏览器，最终显示在用户屏幕上。

在支持ASP的Web服务器中，一个虚拟目录及子目录下所有的ASP文件构成一个ASP应用系统，Web服务启动后，可以创建Application对象，它相当于编程语言中共享的全局变量，可以在任何一个访问服务器的ASP页面中引用。ASP还可以在服务端创建与用户关联的Session对象，该对象既可用于保存与用户相关的参数(如用户名、IP地址等)，也可用于保存其他对象，完成其所承担的任务。而对于其他用户来说，该Session对象是不可见的，可以把Session对象看作为编程语言中的过程变量。此外，通过ASP提供的数据库访问组件，可以高效地实现对数据库的操作。ASP是一个开发复杂Web应用网站系统的成熟技术与环境。

ASP技术最初只能在Windows NT的IIS环境中使用，之后推出的iASP脚本解释引擎系统，使ASP可以在其他操作系统（如Unix、Linux、Netware）及相应服务器的网站上使用，从而成为一个跨平台的Web应用支撑。此外，最近流行的与ASP异曲同工的、在Unix环境中运行的PHP技术也是一种脚本解释引擎系统，大大方便和加强了Unix环境信息网站的应用开发。

4.2 信息的存储

对于安全机制较完善的信息系统来说，无论是用户注册资料还是在网上发布的各类信息都应使用数据库来存储和管理，从而在减小文件管理工作量、保障系统高效运行的同时，提高了信息系统的安全性。

例如，在用户注册库中，每个用户的注册信息占一条记录，与用户关联的用户名、密码、IP地址等信息分别存储在相应字段中，便于快速查找和比对。

在网上发布的各类信息均采用数据库进行存储，用户发布的信息应附上发布人姓名、发布时间、发布机器的IP等信息，信息发布范围以及指定的阅览人姓名等也应安排相应字段来存储。如此处理，不仅便于对信息的查询、统计，也增强了网站信息来源的可追溯性。

4.3 用户权限控制

在上述基础上，实现用户权限控制是一件不太困难的事。

当用户登录网络后，系统自动生成用于保存用户姓名的Session对象，该Session对象在其有效期内将伴随着用户在网上的一切活动，从而使系统对该用户的跟踪和限制成为可能。例如，当用户欲阅览某篇信息时，系统将首先获得该Session对象用户的阅览权限，当用户阅览权限低于该信息发布时设定的权限值时，用户将不能阅读该信息的正文内容。反之，系统将从数据库中提取该信息的正文部分、动态生成HTML网页发送给该客户机用户浏览。更彻底的处理方法是：不允许用户阅览的信息，该用户甚至连信息标题也看不到。

用户发布权限的控制也基于同样的工作原理。当用户激活信息发布向导时，系统对伴随该用户的Session对象进行检查、归类，并将动态生成的、与该用户发布授权相符的信息发布界面发送给用户，使得用户只能在许可的信息发布范围从事信息发布活动。■

参考文献

1 《Active Server Pages (ASP) 2.0网页设计手册》清华大学出版社

2 《Active Server Pages & WEB数据库》人民邮电出版社