不同的资源使用不同的访问权限的。你可能已经注意到了，图 12-2b 的 WWW-Authenticate 质询中包含了一个 realm 指令。Web 服务器会将受保护的文档组织成一个安全域（security realm）。每个安全域都可以有不同的授权用户集。

比如，假设 Web 服务器建立了两个安全域：一个用于公司的财务信息，另一个用于个人家庭文档（参见图 12-3）。不同的用户对各个安全域的访问权限是不同的。公司的 CEO 应该能够访问销售额预测资料，但不应该允许他访问员工和其家人度假的照片！

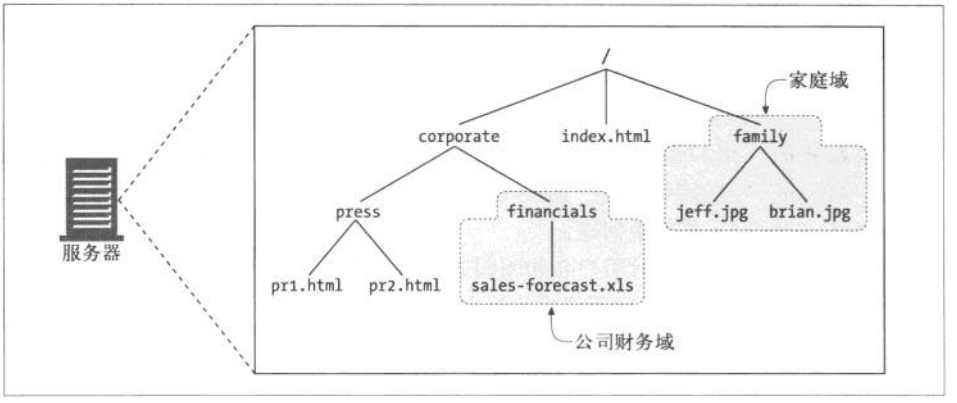

图 12-3 Web 服务器上的安全域

下面是一个假想的基本认证质询，它指定了一个域：

```
HTTP/1.0 401 Unauthorized
WWW-Authenticate: Basic realm="Corporate Financials"
```

域应该有一个描述性的字符名，比如 Corporate Financials（公司财务资料），以帮助用户了解应该使用哪个用户名和密码。在安全域的名称中列出服务器主机名也是很有帮助的——比如，executive-committee@bigcompany.com。 280

12.2 基本认证

基本认证是最流行的 HTTP 认证协议。几乎每个主要的客户端和服务器都实现了基本认证机制。基本认证最初是在 HTTP/1.0 规范中提出的，但此后被移到了 RFC 2617 中，它详细介绍了 HTTP 的认证机制。

在基本认证中，Web 服务器可以拒绝一个事务，质询客户端，请用户提供有效的用户名和密码。服务器会返回 401 状态码，而不是 200 状态码来初始化认证质询，并