# Netware 网络安全性的考虑

中国电子设备系统工程公司 刘德贵

**摘要**：*Netware* 网络是面向客户／服务器结构的，其网络安全性从两方面进行授权考虑：首先是用户向网络系统注册权限；其次是网络服务器文件管理系统的访问权限。

## 一、注册权限

向 Novell 网络注册要解决两个问题，一是用户注册名称；二是使用口令字（又称通行字）。在 Netware 中用户名和口令字的设置都受网络控制程序(Supervisor)的控制(以下简称网控程序)。

在用户注册过程中 Netware 采用了四种安全措施：

**1.口令字进行身份限制**

网控程序有许多方法控制口令字的注册过程，系统采用 SYSCON 菜单方式对用户进行身份的控制：

(1)允许用户修改口令，规定用户是否可改变自己的口令字。

(2)申请口令字，特殊用户可申请各种设置的口令字。

(3)最短口令字长度，口令字最短要求 5 个字符，最长为 128 个字符。

(4)定期改变口令字，用户可规定口令字使用限期，网络口令字限期缺省值为 40 天。

(5)缓期注册，口令字到期，缺省值可缓期六次注册。

(6)申请唯一口令字，系统只允许用户从近期用的 8 个口令字中确定一个使用。

**2.站点限制**

网控程序可以管理和控制用户注册的物理站点数目。该站点控制功能还可使临时用户注册到盘系统工作区进行工作。注册到非网控区系统的用户也可使用该区文件工作。用 SYSCON 菜单工作用户，要规定站点号只限于单个用户使用。

**3.时间限制**

对单个用户和所有网络用户都可用时间限制的条件。系统中缺省时间限制条件可由系统管理员对所有用户进行设置，单个用户的时限条件可由用户自行决定。该时限操作均在 SYSCON 菜单工具中完成。

**4.入侵者检测及加锁**

为防止入侵者不正常的用户注册，系统在 SYSCON 菜单中设有入侵者检测控制机制。系统没有加锁防入侵机制时，对非法入侵的次数，可进行记录并防止入侵。

## 二、委托权限

该权限是对系统的网络文件服务器的授权规定，具体说也就是对指定文件目录的授权。这种授权机制是：目录一旦授权，即可扩充到子目录，在另一层重新规定授权的项目。网控程序对所有目录拥有一切权力，可以授给用户的权力如下：

(1)读操作：从打开文件中读出。拥有此权的用户即可运行程序目录中的程序，或在数据目录中查看数据文件的内容。

(2)写操作：可向打开的文件写入内容。拥有此权的用户即可改变数据目录中某个文件的内容。

(3)打开操作：可打开当前文件。拥有此权的用户即可运行程序目录中的程序或打开数据目录中的数据文件。

(4)创建操作：可创建新文件。拥有此权的用户可在数据目录中创建新文件，或在当前目录中创建子目录。

(5)删除操作：可删除作文件。拥有此权的用户可以删除文件和子目录。还可删除由程序建立的程序目录和临时文件。

(6)父权操作：拥有此权的用户可创建、更名、删除子目录；同时还可在目录或子目录中给用户设置授权和目录授权。



© 中国科学院软件研究所 http://www.c-s-a.org.cn

(7)检索操作：允许用户对文件列表。

(8)修改操作：允许修改文件属性。

对以上这些用户的委托授权，网控程序还要给用户访问目录以同样授权，使其具有最大权屏蔽。在使用目录时，用户拥有的有效权在两方面：一是各种授权的组合；二是由网控程序提供最大权屏蔽，这样用户在某一期间可保护授权，以屏蔽对授权的破坏。

团体用户也可以授权，网控程序可为团体用户目录创建授权。

所有用户都应了解自己的授权范围，根据权限工作可防止对无权的目录和文件进行不正常的操作。

## 三、目录访问

Netware 对目录的安全性设有两种机制，一种是限制所有用户的授权；另一种是用户可隐藏目录。

**1.目录的最大授权**

网控程序虽然对目录的任何一种授权都可以消除，但用户对某些目录授权可拥有最大权屏蔽，用户可以绝对保持具有此种权力。这样用户对目录的权力除可拥有父权的绝对权力之外，还可以利用最大权屏蔽方式取得绝对的授权。

对目录拥有父操作授权的用户都可有权使用网控程序改变最大权屏蔽的设置。网控程序对父权的授予应该非常慎重。因为拥有父授权的用户能够复任何原来被取消的目录授权。

**2.目录属性**

目录本身可具有属性。父目录对属性有修改权。系统命令 FLAGDIR 可以确定以下属性：

(1)标准情况：说明无属性设置。

(2)隐藏情况：指隐藏目录，目录列表时任何用户都不能看到该目录，但知道目录名时，用户仍能改变此种目录。

(3)系统情况：指出由系统使用的目录，目录检索过程中，其内容不进行显示。

(4)保密情况：除非用户拥有检索权限，否则目录的内容不能查看。

## 四、目录的有效权

用户拥有对目录的有效权是指具有最大权屏蔽和用户授权两种情况的组合。用户目录的有效权决定方法如下所示：

| | Read | Write | Open | Create | Delete | parte | Serarch | Modify |
|---|---|---|---|---|---|---|---|---|
| 授权 | R | | O | | D | P | S | |
| 最大权蔽 | R | W | O | C | | menta | S | |
| 有效权 | R | | O | | | l | S | |

了解用户所拥有的目录有效权，随时掌握目录授权情况都是非常重要的，以防丢失权力。

**1.有效权的重要性**

在网络环境下工作时，大多数用户使用数据目录中的应用程序进行工作，不只是使用应用程序所在的目录。这就是说用户对数据目录和程序目录需有不同的授权。

(1) 程序目录：用户必须能执行程序目录中的文件，运行程序的最小权力是读、打开和检索。

(2) 数据目录：由于文件需在数据目录中创建和修改，用户必须拥有读、写和打开的权力。根据用户类型的不同也可有删除和创建权。

在 Netware 操作系统中执行各种任务时所需有效授权如下：

| 工作任务 | 授　权 |
|---|---|
| 读文件 | O,R |
| 写文件 | O,W |
| 创建并写文件 | W,C |
| COPY 或 NCOPY 文件到目录 | D,W,C |
| 作所目录 | C,P |
| 取消空子目录 | P,M,D |
| 检索目录 | S |
| SRO 到 SRW 中改变文件 | M,S |
| 重命名文件 | R,W,M |
| 改变目录的最大权屏蔽 | P |
| 改变授权 | P |
| 删除文件 | D |

## 五、文件访问

目录中的文件可以用各种改变文件属性的方法加以保护。利用文件属性可以防止对文件偶然的清除或修改。



© 中国科学院软件研究所 http://www.c-s-a.org.cn

Netware 网络对文件属性可用 FLAG 或 FILER 命令规定，这些文件属性如下：

| 属 性 | 作 用 |
|---|---|
| 只执行 | 防止 EXE 和 COM 文件被修改或拷贝，只能由网控程序规定 |
| 只读 | 防止文件被修改 |
| 只写 | 允许用户读出和修改文件 |
| 不共享 | 一次只有一个用户使用不共享文件工作 |
| 标准 | 标志文件作为不共享和读/写操作 |
| 隐藏 | 有些属性文件不能在列表中出现 |
| 索引 | 索引大型文件的 FAT 入口，以改进硬盘驱动器存取 |
| 修改 | 修改文件的属性、文件备份时，只备份已修改过的文件 |
| 系统文件 | 有系统属性标志的文件，列表中不出现 |
| 事务性文件 | 指出文件由事务处理跟踪系统来保护文件 |

## 六、Netware 386 安全性改进

Netware 386 对网络控制程序的能力有了改进和提高，实现了有效和透明的网络安全性。对目录、子目录和其它任何组合的文件均可给用户授权，允许用户在安全条件下访问资源。以下是 386 网络操作系统中对目录权和文件授权的规定：

| 授 权 | 作 用 |
|---|---|
| 读 | 目录授权:用户可打开和读出在规定的目录和子目录中的文件。文件授权:用户可打开和读出所指定的文件 |
| 写 | 目录授权:用户可打开和写入目录和子目录中的文件文件授权:用户可打开和写入所指定的文件 |
| 创建 | 用户可建立新文件和子目录 |
| 消除 | 目录授权:对目录授权可取消文件和子目录文件授权:用户可删除指定的文件 |
| 目录扫描 | 用户可看到目录名(文目录) |
| 文件扫描 | 用户可看到文件中的文件名，拥有文件授权的用户可看到规定授权的文件名 |
| 访问控制 | 目录授权：用户可修改权列表，并继承该目录的授权屏蔽及有关所有孩子子目录及文件，但用户不能使自己拥有不准备授予的权力文件受权:用户可修改文件受权表，并继承权力屏蔽 |
| 网控程序 | 目录授权:用户对该目录拥有一切权力，及所有孩子子目录和文件。可允许网控程序向目录中的用户和孩子子目录及文件授权。用户对孩子目录和文件拥有一切继承权屏蔽。<br>文件授权:用户拥有规定文件的所有权力 |
| 修改 | 目录授权:用户可改变目录的名称和属性以及所有孩子子目录<br>文件授权:用户可改变规定文件的名称和属性 |



© 中国科学院软件研究所 http://www.c-s-a.org.cn