

Wolfgang Winter and Ludwig Huber

21 CFR 第 11 部分在分析实验室中的实施

第 2 部分：系统与应用的安全

如何确保只有经过授权的人，才能进入系统获取数据？你是否拥有自己的电子签名？如何确认操作者不会使你的数据无效？你的公司是否符合 FDA 法规要求？本文将阐述 21 CFR 第 11 部分中有关电子签名和记录方面的内容。

Wolfgang Winter *is product manager, data systems, and corresponding author* ***Ludwig Huber*** *is worldwide product marketing manager, HPLC, at Agilent Technologies GmbH, PO Box 1280 D-76337, Waldbronn, Germany, +49 7243 602 209, fax +49 7802 981 948, ludwig_huber@agilent.com.*

安全进入机制的目的是防止未授权的人进入系统，并对其中的记录进行更改和删除。它通过信息系统中采用的某种安全机制，使用备份和强化控制方法和策略来实现。Biopharm讲述了对于分析实验室电子签名和记录的总体要求(1)。其中包括在分析实验室中实施无纸化记录系统的关键点。本文将对安全进入、用户权限和审计追踪提供参考。阐述如何检查实验室计算机有关安全机制的设定和密码设置的策略。如果色谱数据系统没有使用安全进入机制，那就需要通过行政手段来对数据的安全进行管理。授权进入的重要性在于不仅要确保保密性，同时要消除人为错误和偶然的数据丢失。

安全进入机制

安全进入 建立严格的规程，规定只有经授权的人才可以进入公司的信息系统(2)。对于计算机系统，从两个方面来实现：物理安全和逻辑安全(3)。实验室要控制非有关人员的进入。但对于制药企业，很难控制未经授权的人走进质检室。那是否意味着不该进入公司数据系统的人，可以检查甚至假造数据记录？如果没有安全机制——内置的数据系统逻辑安全体系，系统数据的误用、出错和伪造是不可避免的。松散的安全机制会影响药品生产系统的质量，针对这样的情况，FDA已作出严格规定。FDA 警告：

> “不能对 21 CFR820.40 所要求的文件控制建立相应的管理规程；没有进行授权检查，来确保只有经授权的人才能进入系统修改文件。例如：“用于生产的仪器和设备的工程图纸以AutoCAD格式存储在台式计算机中，计算机未采取措施防止未授权人的进入对图纸的修改(4)。”

用户ID 负责管理信息系统的IT专员应指定进入系统人员的资质。现在的操作系统可以实现多种安全措施。但在实施时需要科学谨慎的管理方法和适当的安全设置。如果没有足够的安全和密码策略，没有进行及时升级（又叫补丁，可修正先前版本的缺陷）和正确的设置，即使是像 WINDOWS NT 这样具有完善安全体制的操作系统都可能会变得不安全。

安全进入信息系统需要*用户帐号*。每个被授权人都会得到一个用户名或用户ID以及密码来登录系统。分配授权书后，系统管理员使用约定协议——通过使用个人姓和名的足够字母将每个人与一个ID相关联，使得这个ID在系统中具有唯一性：例如在 UNIX 系统中，某用户的登录名是“wwinter”，此用户ID将结合一个只有本人知道的密码，用户ID和密码的结合体在此计算

机系统中就是唯一的，因此该结合体与此用户的手写签名具有同等效力。

大部分操作系统中采用用户ID与密码的结合方式，并由IT部门实施。IT部门不需要重新设计数据系统，就可以自动实现用户鉴别。符合21 CFR第11部分的理想数据系统将使用操作系统提供的安全机制。可以避免做很多额外的工作。

授权 安全操作系统一般都使用“许可”机制，允许或禁止每一个用户访问特定的记录、文件和程序。许可机制确保用户能修改自己的记录，但是只能读(不能修改)其它用户的记录。理论上，该机制能通过管理个人文件和目录来实现。实际上许多色谱数据系统都需要系统管理员，对本地和文件服务器上的个人文件和目录的访问许可进行控制和管理。使用户配置文件非常重要。

用户配置文件的角色 用户配置文件在操作系统，特别是NT中对于统一管理不同任务、不同责任和培训级别的的用户来说非常重要。完善的配置文件，能够限制个人数据只能进入到指定服务器、程序和文件中。在共享私有数据的同时，为数据提供保密性和完整性。系统管理员通过快速创建和实施配置文件来进行管理。

用户配置文件，对于数据系统来说终究是外部方法。数据系统内部记录（原始数据和元数据）的固有独立性使得从外部进行管理非常困难。数据系统必须通过使用如何将个人信息联结在一起的内在逻辑性，来管理记录的完整性与安全性。否则只能依靠系统管理员有关数据系统的知识和经验，来保证结果和原始数据的完整性。

如果按照21 CFR 第11部分的规定选择数据系统，此数据系统必须具备电子记录、电子签名及对文件进行维护和归档的功能，数据系统的供货商需要提供数据系统的组织和修订计划。某些数据系统仅仅依靠标准文件服务器的功能，手工或半手工进行数据组织，与完整的数据组织系统相比，这些系统更容易受到人为错误的影响。

密码策略 多人共享密码时，用户鉴别和保密就会受到威胁。下面引用FDA的一封警告信来说明一些不符合第11部分要求的错误。

其他员工使用一位员工的用户名和密码来进入数据管理系统。在检查过程中，没有自己用户名和密码的员工，通过使用别人的用户名和密码进入数据管理系统。有3位前雇员，已分别于1997年和1998年辞职，却在1999年3月8日进入非公开的数据管理系统(5)。

密码的安全性 在21 CFR 第11部分的11.200章节“鉴定机制和控制”和11.300章节“鉴定代码和密码的控制”中，对使用电子签名的鉴定机制作出要求：鉴定机制应该是“被真实用户所使用”和需要“进行管理，确保试图使用非真实本人的电子签名需要两个或更多人的协作”。

要满足FDA要求，必须实施适当的策略来保证鉴定代码的安全性、完整性、真实性和保密性。

有时用户很难记住他们的“安全”密码。如果密码容易记住，很可能被其他人猜到或通过黑客程序来破译(6)。早期的安全操作系统，根据系统管理员所制订的密码策略非常安全。但普通用户不得不把密码写下来才能记住。因此必须找到一个折中的方法，确保个人密码可靠性的同时，还便于用户使用。

NT操作系统支持*帐户策略*。帐户策略在系统中为所有用户帐号制定密码规则。它特别引入了由于多次非法登录而锁定用户帐号的功能。帐户策略的重要方面是使用普通方法就可以进入所有需要的设定。

用户帐号管理通常由公司IT部门的系统管理员负责。如果实验室数据系统的内在安全设计，没有与操作系统的安全机制联系在一起，系统管理员必须承担双份责任——同时管理操作系统和实验室数据的用户帐号和密码。与操作系统相比，实验室数据系统不提供或仅提供很少的帐户管理策略，实施21 CFR 第11部分比较困难。所以购买数据系统之前，必须检查供货商所提供的不同帐号管理策略，供货商所提供的与操作系统安全机制直接联系的解决方法是最实际的。将在后续

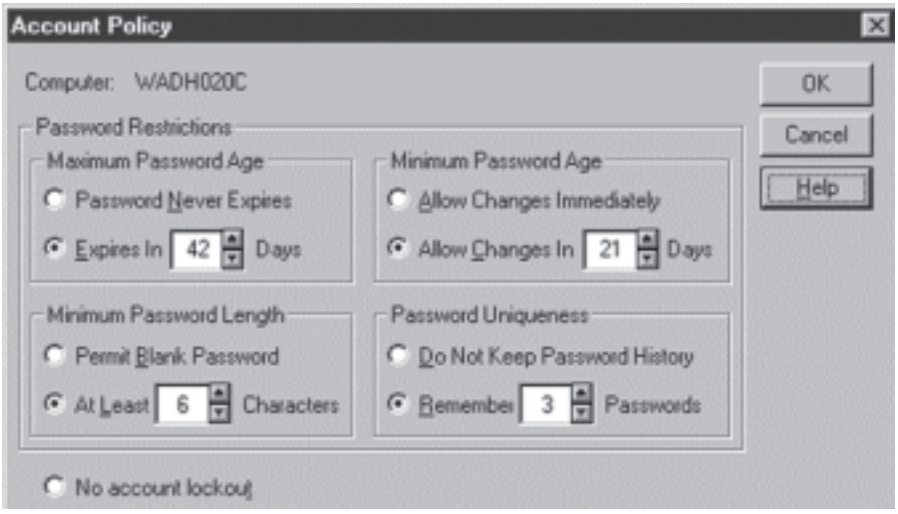


Figure 1. Password policy settings in Windows NT.

文章中讨论实施安全鉴定机制所带来的益处。

实用安全的鉴定系统必须考虑潜在的危险行为，即使用他人的用户名和密码对电子记录进行操作，例如用户登录系统后进行操作，由于某种原因离开计算机时还使系统处于打开的状态。第11部分在第63条注释中提到，降低“不使用自己的电子签名而登录系统和改变已签字确认的记录的可能性”。在法规的第124条注释中，详细的阐明应采取的对策：

> 采取严格的措施防止这种情况的发生非常重要，措施包括：(1) 要求用户在登录系统后，与工作站保持很近的距离。(2) 在固定的时间间隔内如果没有任何输入和其它行为，应自动注销这个用户。(3) 要求用只有经授权的人才知道和能够使用的独立部分，来控制后续的签名(7)。

***SYSTEM** integrity may be impeached even if the electronic records themselves are not directly accessed.*

选择一个数据系统来实施 21 CFR 第 11 部分，应确保数据系统有相应的工具，防止使用其他用户授权书来进行假冒。一些供货商已对此安全条款发表技术声明(8，9)。

合法用户的权限 为符合第 11.10 章节的规定，数据系统将使用什么样的用户进入机制？如果将进入系统的权限授予一组人，而没有按他们的责任、知识水平区别对待，这样做是不全面的。用户也许会不经意地修改系统参数，而影响记录的完整性和安全性。系统管理员应制订书面规程，只有少数人才有系统管理员的权限。对于这种类型的系统登录控制，FDA 在注释的第 83 条进行了解释：

> “控制系统的进入是基本的安全功能，因为即使记录没有被直接登陆，也要怀疑系统的完整性。例如，某人可以进入系统，改变需要密码的条件，或忽略安全机制，使未经授权的人可以修改电子记录或阅读未经授权的信息[7]。”

本规定使用的条件是*授权检查*。那是不是意味着系统管理员必须为每一个用户分配和决定他们进入的权限？根据规则的第 83 条注释，组织机构

> “在对每一条记录进行授权检查时，不必包含授权签字人的名单。例如，一条记录可以与一个代码相连接，这个代码可以识别出对这条记录进行签字的人的头衔和所属的机构组织。因此拥有相应代码的人可以对这条记录进行签字[7]。”

一些实验室数据系统供货商得出结论，数据系统安全性要求应根据用户的工作内容和责任，对他们的权限进行不同的设置。每个公司应根据不同的工作内容，授权不同的权限。需要电子签名的工作可以按同样的方式进行分配。因此这些决定取决于实验室的策略，而不要取决于供货商。

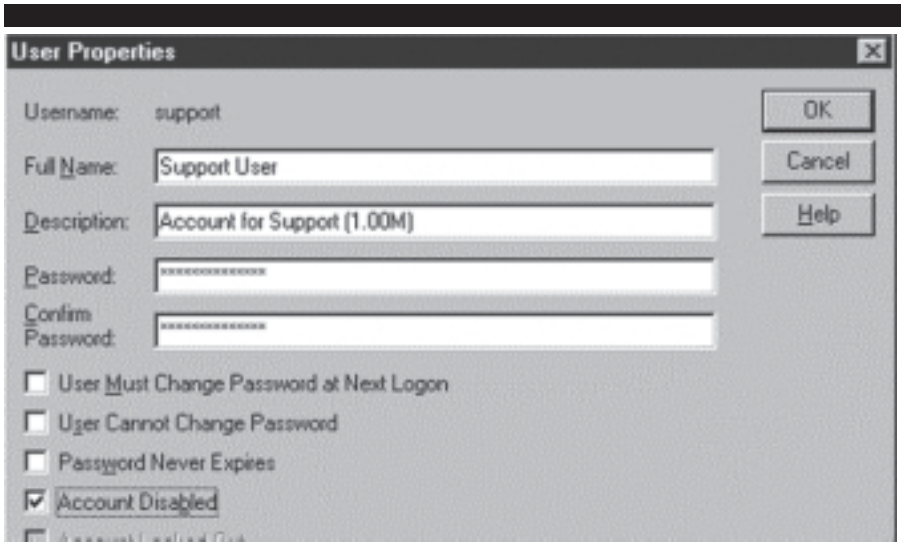


Figure 2. Temporarily disabling a user account in “user manager” of NT.

共享桌面 通常在实验室发现，多个用户操作由一台计算机控制的多台仪器。例如在生产或过程控制的环境下，一台计算机经常控制由多个用户使用的多台色谱仪。如果使用NT操作系统进行用户识别，会带来许多不便，因为注销当前的用户需要关闭当前的任务。如果依赖数据系统，将会影响其它仪器的数据采集。如果使用用户配置文件，建立网络连接，重新开始应用程序，则运行速度慢且不方便。比较好的解决办法是在使用NT操作系统（共享桌面）的计算机上实行登录共享。这要求用户使用自己的用户名和密码登录色谱数据系统。共享的NT帐户没有进入色谱数据系统的权限。这样就可以对每个人使用数据的情况进行追踪和管理。该共享帐户的用户名和密码将不视为电子签名。

远程登录 有些实验室人员需要对数据系统进行远程登录。如果设计合理，即使使用公共设施，远程登录系统完全可以满足 21 CFR 第 11 部分对封闭系统所作出的要求。这样的登录只局限于拥用自己用户 ID 和密码的合法用户。密码的安全可以通过使用一种叫

做 smart-card 的装置得到强化。它能够产生有效期只有几分钟的唯一密码，并且与拨号系统的密码服务相同步，通过对预先设定电话号码的回叫来消除非法用户的可能性。

另一个安全问题是负责登录维护的人员。大部分色谱数据系统的供货商都会在特定的计算机上，为系统工程师设定特定帐号，以便登录系统来安装、调试和维护设定。特别是在NT操作系统中，厂家的维修工程师通常需要系统管理员的权限来安装软件，进行配置或为特定的仪器安装驱动程序。供货商的本意是保护数据，不用或不用共享系统管理员的登录就可以进行服务(根据 21 CFR 第 11 部分的规定，与系统管理员共享登录意味着系统管理员可以否认一项已签字的行为，而声明是其他人做的)。所以有些公司认为设置一个有系统管理员权限的帐户违反数据系统的安全性。

下面推荐一些方法解决这个实际问题

对于需要进入数据系统的维修人员，应该实施**流程控制**。

可以在数据系统中创建**维修人员帐号**。如果出于系统维护的原因，需要为维修人员帐号赋予管理员的权限，只在系统本身创建帐号。如果帐号不用，应该使之失效。只有维修人员需要进入数据系统时，系统管理员才恢复这个帐号。

应该为维修人员帐号建立**用户配置文件**，防止他们进入保密的数据或文件。

如果数据系统允许配置**特定用户权限**，应在服务器帐号中使之失效。因为允许删除、批准或作废结果和修改方法，会影响计算机数据的安全性和完整性。如果工作需要，维修工程师需要与数据安全性有关的系统管理员的权限，那他的工作必须**在系统管理员的监督下进行**。如果供货商的代表了解第 11 部分有关数据完整性的要求，接受过**足够的培训**，系统管理员可以预先审阅并同意他将要采取的活动，而不用监督其每一步。

总之，符合 21 CFR 第 11 部分的数据系统可以根据任务的性质，分配特定的进入权限，使得维修工程师不必执行影响数据安全性的操作。例如：在数据系统中，某项特定任务在完成前需要电子签名，如果在开始执行任务时发现了错误，维修工程师可以终止任务或使系统回到实施任务之前的状态。图1是一幅屏幕截图，显示一个维修工程师准备的帐号被取消的NT用户配置文件。

系统评价

评估系统是否符合 21 CFR 第 11 部分的主要步骤

使用数据系统的安全机制来**控制进入**。理想情况下，数据系统应与操作系统的用户帐号数据库联系在一起。

定义、实施和使用密码制订策略来实现保密性和鉴定用户密码。数据系统应该或者允许定义密码制订策略，或者将密码制订策略与操作系统联系在一起。

对于基于生物测定学的鉴定机制，建议等到它们成为操作系统固有的功能或标准配置时再使用。

采取措施防止冒名顶替。如果当前任务超时操作，系统应自动地锁定任务。根据不同任务的需要制订进入权限。为了管理多用户的进入权限，最好按工作性质而不是按个人进行管理。理想的数据系统应可以按用户组来配置权限。

密码制订策略

精心设计的密码制订策略可以使密码泄密可能性降到最低。为建立实用有效的密码制订策略，请参考以下的指导原则：

1. 用户密码不应该其他人知道，其中包括系统管理员。密码制订的一个策略是当用户第一次登录系统时需要更改密码。
2. 密码应该至少包括 6 个字母，但超过 8 个字母又会使密码很难记忆，而且不容易正确输入。
3. 密码应该包括数字、字母和标点符号（; , 。！ -+？ -:）
4. 不要使用个人信息，例如姓名、电话等作为密码，因为这样很容易被别人破译。
5. 密码不应该包括在字典中查到的单词。
6. 密码中同时包括大小写字母将使密码更安全。
7. 一个帐号如果 3 次登录失败，应该被锁住。
8. 应该经常更换密码，例如 6～8 星期。如果在缩短更改密码的时间间隔，用户会觉得很麻烦，他们也许会将密码写下来。好的密码制订策略是使用“密码生命周期”。
9. 应该避免只在两三个密码间往复变化。密码个数应该比允许不成功登录的次数要多（见第 7 条）好的密码制订策略应保证密码在 5 个之内不重复。
10. 只有用户珍惜自己被赋予的授权，密码制订策略才会有效工作。就像FDA所说的，只有每个人都对自己的行为负责，公司的政策才有意义继续存在。如果我被告之我对每条电子记录进行签名时都要负法律责任，我会更加小心的处理每条电子记录。

如果需要共享桌面，色谱数据系统通过用户名与密码组合的唯一性，进行用户鉴别。共享登录将违反签字记录的原则，如果与他人共享登录，则已签字的记录可以随意更改。

实施安全策略为供货商的维修人员建立帐号。如果可能的话，不要影响系统数据保密性和安全性的任务。如果没有维护工作，为维修人员建立的用户帐号应该失效。另外应考虑是否采取额外的控制手段。

近年来由于违反21 CFR的第11部分，FDA发出一些警告信和483s。虽然大部分制药企业将电子记录应用到生产中，FDA明确希望“这些公司应按规范要求逐步采取措施并有相应的实施计划”[5]。在那些旧型号仪器及随时需要更新的系统中尤其是这样[5]。

参考文献

(1) L. Huber, “Implementing 21 CFR Part 11 in Analytical Laboratories: Part 1, Overview and Requirements,” *BioPharm* 12(11), 28-34 (1999).

(2) *Code of Federal Regulations, Food and Drugs*, Title 21, Part 11, “Electronic Records; Electronic Signatures” (U.S. Government Printing Office, Washington, DC). Also Federal Register 62(54), 13429-13466.

(3) L. Huber, *Validation of Computerized Analytical Instruments* (Interpharm Press, Inc., Buffalo Grove, IL, 1995).

(4) *Compliance Policy Guide: 21 CFR Part 11; Electronic Records, Electronic Signatures* (CPG 7153.17) (FDA, Washington, DC) www.fda.gov/ora/compliance_ref/cpg/cpggenl/cpg160-850.htm.

(5) *Gold Sheet* 33(7) (F-D-C Reports Inc., Chevy Chase, MD, 1999).

(6) M.J. Edwards, “The Handy Security Toolkit Revisited,” *Windows NT Magazine* (October 1999) www.winntmag.com.

术语表

安全进入 决定谁可以从本地或网络进入系统。主要通过在线建立某种机制防止未授权人进入系统。大部分操作系统提供几种不同类型的进入权限赋予给特定的用户或用户组。

管理特权或系统管理 是一种责任，它用来维护多用户计算机系统并管理网络权限，例如为特定用户设置新帐号和权限。

应用程序 是一种安装在计算机上用于执行特定任务，并只有少数人被允许使用的软件。

合法注册或冒名顶替 使用他人的用户ID和密码进入网络，来获取他人没有被授权的网络资源，可以是故意的或不是故意的。

审计追踪 由计算机生成并带时间标记的活动记录。第11部分要求审计追踪必须独立于操作者，并且必须捕获与系统相关的所有活动：例如创建、修改或删除记录。

鉴定机制、授权检查或授权签字人 与授权进入网络获取资源截然不同，鉴定程序通常被系统管理员使用，用于确认进入网络系统的人是否合法。FDA说“授权检查”是“确保只有经授权的人才能使用系统，对记录进行电子签名，进入操作系统或计算机系统使用输入输出设备，改变记录或执行操作。”

生物测定学 生物制药科学家也许认为生物鉴别学是对生物现象的一种统计学研究。但从计算机安全角度来说，它是一种鉴定技术。通过对可自动检查的物理特征进行测量来实现，例如指纹、语音或视网膜特征。FDA将生物测定学定义为“基于一个人的生理特征，或者是一个人可测量可重复进行的特有行为，来进行某人身份的确认。”

封闭系统 进入系统时受到控制的一种环境，管理员对系统中记录的内容负有责任。大部分符合FDA规范的公司都属于这个类型。

配置设置 定义组织结构权限是如何设置的，例如一个用户只能读这个文件，但另一个人能执行这个文件，第三个人能往这个文件写数据。

数据完整性 是指数据及其关系的有效性。为了保证电子数据的可靠性和可信性，原始数据、元数据和结果之间的联系必须紧密相关，如果没有数据的完整性，就不可能产生可靠的结果。

使帐号失效 一个用户帐号的进入权限被取消，直到在某一时间又被重新赋予进入的权限。

电子签名、数字签名，或e-sigs 根据FDA的要求，电子签名是指“由个人制作、采纳并授权的任何符号或系列符号化的计算机数据，它具有与个人手写签名同等的合法地位。”数字签名是指“基于密码学的电子签名，它通过一套参数和规则进行鉴定和计算，从而能够对签名者的身份和数据的完整性进行核实。”

密码学 将数据转换成秘密代码是最有效的数据安全措施。未加密的数据叫明文，加密的数据叫密文。

外部或远程登录 远距离登录网络的能力。含有数据的系统叫*主机*，操作者所使用的计算机叫*终端*，终端和与网络直接相连工作站的差别仅仅是较低的数据传输速度。

ID参数 通常以用户ID和密码的形式设置鉴定和授权代码。设置的唯一性使得用户可以进入文件，下达命令或运行程序。

取消连接或锁住任务 在一段时间内没有数据输入的情况下，注销或冻结一个计算机任务。

信息技术(IT) 广义上讲是指管理和处理信息，特别是在大的公司里。也指*信息服务(IS)*或*信息服务管理(MIS)*。

(7) "Rules and Regulations" comment 124, *Federal Register* 62(54) (20 March 1997), pp.13429, from the Federal Register Online, GPO Access, DOCID:fr20mr97-25.
(8) *Implementing Electronic Records and Signatures with Hewlett-Packard's ChemStation*, (Hewlett-Packard, Little Falls, DE, 1998) publication number 12-5966-2315E.
(9) *Using ChemStation Plus to Comply with FDA 21 CFR Part 11*, (Agilent Technologies, Little Falls, DE, 1999) publication number 5968-7930E. ***BP***

术语表(继续)

整体数据组织系统，逻辑安全或内在逻辑 将公司操作系统中的不同应用程序结合在一起，有效地达到鉴定和授权的目的。

注册、登录或使用用户名和密码注册 使用计算机系统识别用户，授权用户可以开始工作的鉴别方法，通常使用用户名和密码。

元数据、原始数据和结果 元数据对于从原始数据生成结果非常重要。色谱包括积分参数和校正表。例如"1000 ÷ 5" =200 这个算数运算，"1000 ÷ 5"是原始数据，在纸上进行的四则运算是元数据，"200"是结果。

开放系统 进入系统时不受系统控制的一种环境，该环境很少或没有安全授权或鉴别。

操作系统或操作环境 是计算机执行任务来最重要的程序，例如接收键盘输入，输出结果到显示器，保存目录和文件，控制诸如象打印机的外部设备。Windows NT, LINUX, UNIX 都是操作系统。

密码破译 理论上说，没有人能猜出密码。但在实际中，人们通常选择容易记忆的密码。例如他们的名字或名字的首字母。密码破译程序试图猜出密码使得未授权的人可以闯入计算机系统。解密者通常是指侵入安全系统的人，而黑客是指更喜欢了解计算机系统或对安全信息搞恶作剧的人。

许可或权限 是指定义或限制用户读、写和执行相关文件、目录和程序的安全代码。例如：一些部门仅仅需要查看数据，另一些部门需要输入数据或运行程序，而其它部门则不能进入数据系统。

认可原则 有能力确保仅仅一个用户可以在计算机系统中获取数据或执行特定任务，而且这个用户已被确认。如果有多个用户进入系统，而审计追踪并不能辨别谁执行了什么操作，那认可原则就被破坏了。

私有数据共享 只有数据的所有者才能进入文件服务器上自己的目录。

脚本或管理脚本 又叫宏或批文件。脚本是可以自动执行任务的一组程序。管理脚本通常为系统管理员提供工具，帮助管理员为系统的安全设定用户权限。

安全机制 是指将数据储存在计算机上不被别人获取的技术。大部分安全措施涉及到加密或密码。

服务器、程序和文件 服务器是指在网络上管理网络资源的计算机或设备。文件服务器存储数据，打印服务器管理打印机，网络服务器管理网络交通，数据库服务器拥有供查询的数据库。程序是指有组织的命令清单（象处方），使计算机以预先决定的方式工作。文件是包含有文件名的数据集合：例如文本文件，数据文件，程序文件和目录文件。

维修服务帐号或服务人员帐号 预先设定在计算机系统中的一个帐号，用于维修人员进入不同机器进行维修工作。

升级版本或补丁程序 修补操作系统缺陷的程序或对先前版本缺陷的报告。它们需要在原有软件的基础上才能安装。

共享桌面、帐号或注册 个人计算机通常被称为桌面。共享个人计算机，帐号或登录违反了认可原则。如果在共享网络资源时审计追踪不能辨别共享信息，那电子签名就是无效的。

任务进入权限或由角色进入权限 这是系统管理工具，用于设定用户配置文件，分配用户到用户组，然后给这个组的所有成员分配特定的权限。例如："经理组"也许只有阅读 QA/QC 文件的权限。但是作为"发酵组"的成员，发酵部门的经理可以有写入的权限。根据任务或工作来分配权限，可以授权用户只能使用与他们工作有关或工作需要的网络资源。

Copyright Notice *Copyright by Advanstar Communications Inc. Advanstar Communications Inc. retains all rights to this article. This article may only be viewed or printed (1) for personal use. User may not actively save any text or graphics/photos to local hard drives or duplicate this article in whole or in part, in any medium. Advanstar Communications Inc. home page is located at http://www.advanstar.com.*

©Reprinted from BIOPHARM, January 2000 AN ADVANSTAR PUBLICATION Printed in U.S.A.

出版号：5980-1306CHCN