访问控制

ISO17799十一个领域之七：访问控制

访问控制是对主体(Subject)访问客体(Object)的权限或能力的一种限制。

所谓主体是指可以访问对象的活动实体，例如需要访问数据资源的管理员，或修改数据的某个程序的某一进程等；所谓客体是指含有信息并接收访问的实体，如文件、程序、系统、信息处理设施等。

在信息安全学中，访问控制一般分为逻辑访问控制与实体访问控制（又称物理访问控制），逻辑访问控制是指：对主体通过计算机终端及网络来使用信息处理系统并访问数据资源的行为进行控制；实体访问控制是指：在存放有信息处理设施的重要区域，对进出人员进行限制。

在这里，ISO17799所说的访问控制主要是指逻辑访问控制，在网络广泛互联的今天，采用技术与管理手段建立逻辑访问控制己是保障信息安全的重要手段。关于实体访问控制在第五部分“实体与环境安全”中的“安全区域”中己有描述。

ISO17799对访问控制以下几个方面进行描述：访问控制的业务需要、用户访问管理、用户责任、网络访问控制、操作系统访问控制、应用系统访问控制、检测系统的访问与使用、移动计算与远程工作。

1、控制目标－访问控制的业务需要

目标：控制对信息的访问

 根据业务和信息安全的要求，组织应当控制对信息和业务应用系统的访问。应当把信息发布和授权的策略考虑在内。

 组织的业务运作需要信息的支持，一方面组织要充分利用信息资源，另一方面要对信息的使用进行一定的限制，以达到保护信息资产的目的。对信息的保护程度要取决于业务的要求及信息安全的要求，组织应当建立明确访问策略，为信息的访问控制提供指导。

控制措施－建立并实施访问控制策略

 ==> 应当清楚地定义组织业务对访问控制的要求并使之正式成文。

 应当定义并记录下对访问控制的业务要求。在访问控制策略说明中，应当清楚阐明访问控制规则及个人用户和群体用户的权限。用户和服务提供商都应当提供一份对访问控制所要满足的业务要求的详细说明。访问策略的结构如表所示：

访问控制策略 所要控制的信息(数据、系统、网络)

 访问控制规划

 用户或用户组访问权限

 其他访问安全要求

2、控制目标－用户访问管理

目标：防止对信息系统的未经授权的访问

 应当建立正式的程序来控制对信息系统和服务的访问权限分配。

 这些程序应当覆盖用户访问全过程，从新用户的最初注册到不再需要访问信息系统和服务的用户最终的注销。并特别注意控制特权访问权限的分配。

 为防止对信息系统的非授权访问，组织应根据访问控制策略的要求，对用户(包括内部用户和第三方用户)访问权限进行管理。管理内容包括用户注册与解除注册过程、特权管理、口令管理与用户访问权限的评审。

控制措施－用户注册

 =>应建立正式的用户注册及注销的程序，对用户访问信息系统和服务的权限进行控制。

 为确保访问信息系统和服务的用户的合法性，组织通过建立一个正式的用户注册和解除注册的授权程序，对用户访问信息系统和服务的权限进行控制。

控制措施－特权管理

 ==>对于特殊权限的分配及使用，应加以限制及控制。

 应当严格限制系统特权的分配和使用。特权是指用户超越系统控制或应用控制而拥有对信息系统的特殊访问权限。例如，系统管理员就拥有特权，其访问权限高于一般用户，系统管理员可以对系统参数进行配置或对一般用户的访问权限进行控制。

 对系统特权的不当使用是导致系统产生故障及引起攻击的一个主要因素。应当通过正式的授权程序来控制对特权的分配。

控制措施－用户口令管理

 ==>对于口令的分配，应通过正式的管理流程加以控制。

 在用户访问信息系统和相关服务时，口令是用来确定用户身份的常用方式，并且是控制访问服务和访问数据的关键。口令的发布应受到控制，否则容易产生许多安全问题。如口令的泄露、口令的共享会导致信息泄密，信息被非法修改，造成数据损失及安全审计性被破坏。因此组织应当通过正式的管理过程来控制口令的分配。口令管理还需接合用户责任及控制软件的使用，其一般过程如下有所示：

 控制内容 控制方式

 用户口令管理 用户口令分配策略

 用户责任 遵守选择与使用口令的规则

 口令管理系统 操作系统及应用系统对口令管理的支持

控制措施－用户访问权限的评审

 ==>为确保访问控制的有效性，管理层应定期对用户的访问权限进行评审。

 为了能对数据和信息服务的访问进行有效控制，管理层应当建立正式的程序，来定期评审用户的访问权限。对于评审周期一般有以下要求：对普通用户的访问权限，建议每6个月评审一次，并在做任何改动后进行复查；对特权访问的权限，建议每3个月评审一次；对发现的问题要及进采取纠正措施。

3、控制目标－用户责任

目标：防止未经授权的用户访问。

 得到授权的用户的合作是有效的安全管理的基础

为了维持有效的访问控制，应当让用户知道他们的责任，尤其是有关口令使用和用户设备的安全方面的责任，并严格遵守有关安全规定。

控制措施－口令的使用

 应该要求用户在选择及使用口令时，遵循良好的安全惯例。

 用户应当按照良好的安全操作规程来选择和使用口令。

 口令提供了一种验证用户身份的手段，从而建立了对信息处理设备和服务的访问权限。 应当建议所有的用户：保护口令的保密性；避免在纸张上保留口令记录，除非可以对其安全存放；只要有系统或者口令可能被侵害的迹象，就更改口令；选择的优质口令至少要有8个字符的长度；定期更换口令或者根据一定量的访问次数来更改口令（特权帐户的口令应当比普通帐户口令更改的更为频繁）；避免重复或者循环使用旧的口令等措施。

控制措施－对无人值守设备的管理

 ==>用户应当采取适当的措施，保护无人看管的设备。

在用户区安装的设备，例如工作站或者文件服务器，可能需要特殊的保护，以防止在较长的无人值守时间内被非法访问。如：设备使用完会话还未结束时，要将活动的对话终止；使用带口令保护的屏幕保护程序；在PC机和终端不使用时，要采用实体防护措施，如锁在受保护的工作间中或专用的柜子中。

4、控制目标－网络访问控制

目标：保护组织的网络服务正常工作

 应当控制对内部和外部网络服务的访问，确保对网络具有访问权限的用户不损害系统的安全。

组织在享受网络服务的方便与快捷的同时，也存在内部与外部、无意与恶意的对组织网络的未经授权的访问。因此，为保护网络服务的安全，要对内部和外部网络服务的访问加以控制，要确保：在本组织的网络和其它组织的网络，例如公共网之间有适当的接口；对用户和设备的适当的授权机制；对用户访问信息服务的控制等。

控制措施－网络服务的使用策略

 ==>用户应该仅能访问已获授权使用的服务 。

 组织应当制定明确的策略，规定对网络服务的访问原则：界定那些网络和网络服务允许访问；确定谁可以访问那些网络和网络服务的授权程序；制定对网络连接和网络访问服务的管理措施和程序；网络服务使用策略应当与组织的业务访问控制策略相一致。

控制措施－外部连接用户身份识别

 ==>应对远程用户的访问进行身份认证。

 外部连接可能导致针对信息系统的未经授权访问，例如外部拨号访问。因此，应当把远程用户的访问置于比其它方式更为严格的保护之下。例如使用先进的密码技术来提供对用户身份的强认证。对于可能的各种外部连接，先通过风险评估来确定所需保护等级，然后采取相应的加密认证方法。

控制措施－对网络设备进行身份识别

 ==>应考虑对网络设备进行自动身份识别，将其作为鉴别来自特定位置和设备的连接的有效方法。

如果通信只能从特定位置或设备进行启动，则应当对设备进行身份识别。识别时使用设备标识或设备连接标识可用于指示此设备是否允许被连接到网络。如果存在多个网络，尤其是如果这些网络有不同的敏感度，这些标识符应清晰的指明设备允许连接到哪个网络。可能需要考虑设备的物理保护以维持设备标识符的安全。

控制措施－远程诊断端口的保护

 ==>应控制对诊断和配置端口的物理访问和逻辑访问。

 对诊断和配置端口首先要采取加锁保护、机房或设备间隔离等措施。

 为了方便维护工程师的远程使用，许多计算机和通信系统都安装了远程拨号诊断设施。如果不加保护，这些诊断接口就为未经授权的访问提供了途径。因此，应当建立适当的安全机制对其加以保护，例如采用口令和程序保护对此端口的使用；当端口不需要使用时，使其失效；每次使用端口时都相应授权与日志记录等。

控制措施－对网络进行隔离

 ==>应采取适当方式对信息服务、用户及信息系统进行隔离，以减少非授权访问的风险

由于某些网络的敏感性和重要性，应当考虑在网络中引入管理措施对不同的信息服务、用户和信息系统进行分离。大型网络的安全管理方法之一就是将其分解为独立的逻辑网域，例如组织的内部网域和外部网域, 每个域都建立确定的安全边界，并加以保护。

可以在两个域之间安装一个安全网关，来实现上述的安全边界，这一安全网关经过定制，可以过滤不同域之间的通信，并能够按照组织的访问管理措施，限制未经授权的访问。这种安全网关的一个例子就是我们通常所说的防火墙。

控制措施－网络连接的控制

 ==>应限制用户联接共享网络的能力，并与业务应用系统的访问控制策略和要求一致。

共享网络，特别是那些跨越组织界线的广域网，需要对用户的网络连接能力进行控制。，例如要对以下连接进行限制：消息传递，例如电子邮件、文件传送、交互式访问、应用访问等。这种控制措施可以通过网关，按照预定义规则(IP访问控制列表)过滤通信量来实现。过滤规则要与访问策略一致，并随访问策略的变化而修订。

控制措施－网络路由的控制

 ==>应对网络进行路由控制，以确保信息联接和信息流不违反业务应用系统的访问控制策略。

共享网络，特别是那些跨越组织界线的广域网，需要进行路由控制，以确保计算机连接和信息流不会破坏组织的访问控制策略。路由选择控制应当基于对IP源地址和目标地址的检测机制。如：网络地址翻译(NAT)对于隔离网络和防止路由从一个组织的网络不受控制地延伸到另一个网络，是一种非常有效的机制。

5、控制目标－操作系统访问控制

目标：防止对计算机非授权访问。

 操作系统的安全设施应当用于限制对计算机资源的访问。

 组织要采用一定的安全设施来限制访问计算机资源，这些设施应当能够做到：鉴别和验证身份；记录对系统的成功访问和失败访问；提供适当的授权方式；如果使用了密码管理系统，应当能够确保使用的是优质密码；在适当的地方，限制用户的连接次数。

控制措施－安全登陆程序

 ==>使用安全登录程序访问信息服务，可以减少非授权访问的机会。

 对信息服务的访问应当由一个安全的登录程序获得，这一登录到计算机系统的程序要能降低非授权访问的机会。为了避免被未经授权者利用，登录程序只会向用户透露出最少的系统信息。

控制措施－用户身份标识与鉴别

 ==>所有用户应有唯一的标识码专供其个人的使用，以便各项活动可以追溯至应负责的个人。应使用一种适当的认证技术以真实地鉴别使用者的身份。

所有的用户（一般用户、网络管理员、系统程序员和数据库管理员等）应当有唯一的标识（用户ID）供他们个人并且只供他们个人使用。因此，任何计算机活动与事件都可以追踪到负有责任的个人身上。用户ID不应当显示出用户的特权等级，例如管理人员、监控人员。

有各种身份鉴别程序用来证实用户身份，如口令就是一种非常通用的进行识别和鉴定（I&A）的方法。也可以通过加密技术和认证协议的方法来实现鉴别。

用户所拥有的实物(像存储标识或者用户拥有的智能卡)也可以用来进行识别和鉴定；利用个人唯一特征或属性的生物测量技术也可以用来鉴别一个人的身份。将鉴别技术和管理机制妥善地结合到一起能够得到更为强大的用户身份鉴定能力。

控制措施－口令管理系统

 ==>口令管理系统应提供有效的、交互式的设施以确保使用优质的口令码。

 口令是验证用户访问计算机权限的主要形式之一。口令管理系统应当提供一个有效的、交互的口令管理方式，来确保提供优质口令。用户口令可以通过独立主管来分配，大多数情况下，密码是由用户选择和维护的。

控制措施－限制系统实用工具的使用

 ==>系统实用工具的使用应加以限制并严格控制。

 大多数计算机安装有一个或者多个系统实用程序(UtilityProgram)，它们可能超越系统和应用程序的控制，因此，限制并严格控制对它们的使用是十分重要的。

控制措施－不活动的会话应在一个设定的不活动周期后关闭。

 ==>超过一段设定的不活动的时限时，系统应首先清空会话屏幕；当超时更长时，应关闭应用和网络会话。

 为了防止非授权用户的访问，高风险地区（例如在组织的安全管理之外的公共场所或外部地区）的终端应当在定义的不活动时间后关闭。另外还可以应用一种有限形式的终端时限功能，即清除终端屏幕内容（如启动带口令的屏幕保护程序或不进行操作时立即启用操作系统锁屏功能）来防止非授权访问，但此时并不关闭应用程序和网络对话。

控制措施－连接时间限制

 ==>应使用连接时间的限制，以提供高风险的应用程序附加的安全保护 。

对连接时间的限制为高风险应用程序提供了额外的安全保证。限制终端连接计算机访问的时间，减少了非授权访问的机会。对于敏感的计算机应用程序，特别是安装在高风险区域的终端，应当考虑这种措施。

6、控制目标－应用系统访问控制

目标：防止保存在信息系统内的信息被非授权访问。

 信息系统会受到未授权的访问与修改的威胁，造成敏感信息泄漏或信息的破坏，为防止非授权访问储存在信息系统内的信息，应使用应用系统的安全功能（设施）来限制访问，对软件和信息的逻辑访问应当限制在合法授权用户之中。

 应用系统访问控制应当做到：

 (1) 控制用户对信息和应用系统功能的访问，并要与业务访问控制策略相一致；

 (2) 为任何一个能够超越系统或应用程序限制的实用程序和操作系统软件提供保护，防止未经授权的访问；

 (3) 不损害有共享信息资源的其它系统的安全；

 (4) 只能够向所有权人、或其他授权用户群提供对信息的访问权限。

控制措施－信息访问限制

 ==>对于信息及应用系统功能的访问应依照访问控制策略加以限制。

 按照确定的访问控制策略，应当为应用软件系统的用户包括技术支持人员提供对信息和应用程序系统的访问。如：提供菜单来控制访问应用程序系统功能；通过适当编辑用户文件，可以限制用户对于未得到授权进行访问的信息或者应用程序系统功能的了解；控制用户的访问权限，例如读取、改写、删除和执行等权限等。

控制措施－敏感系统的隔离

 ==>敏感系统要求专有的计算机环境，在专用计算机上运行，仅与可信赖的应用系统共享资源。

 有些应用程序系统对于潜在的损失非常敏感，需要对它们做专门处理。敏感系统的隔离可以采用物理隔离 （专用的运行环境或独立网络）或逻辑隔离的方式来实现。注意以下要点：

 对一个应用程序系统的敏感性应当有清楚的定义，并且由应用系统所有权人把它记录在案；

 当一个敏感的应用系统需要在共享的环境下运行时，应当识别出与其共享资源的其他应用系统，并由敏感信息的所有权人的准许。

7、控制目标－移动计算与远程工作

目标：在使用移动计算和进行远程工作时确保信息安全。

 使用移动计算或远程工作设施时应当考虑在未经保护的环境下工作的风险，并且要考虑到所采用的适当措施。在远程工作时，组织应当为远程工作地点提供保护并且确保对这种工作方式有适当的安排。

控制措施－移动计算和通讯

 ==>应建立正式的策略并实施适当的控制，以防范使用移动计算和通讯设施的风险。

 使用移动计算设备例如笔记本电脑、掌上电脑、膝上电脑和移动电话等的时候，应当特别注意要确保业务信息不受损害。应当采取正式策略来考虑使用移动计算设备的风险，特别是在未加保护的环境之中。

例如，该策略应当涵盖物理保护、访问控制、加密技术、备份文件和防范病毒等等方面的需要。该策略还应当包括把设备连接到网络的规则和建议，以及在公共场所使用这些设备的指导。

控制措施－远程工作

 ==>应开发策略、程序和标准以便授权及控制远程工作。

 采用通信技术使得员工能够在组织之外的远程固定地点工作，对远程工作的适当保护应当防止设备和信息被盗窃、未经授权的信息披露、对组织内部系统的非经授权访问或者对设备的滥用。远程工作不但需要授权还要由管理层进行控制。组织应当开发相应策略、程序和标准来控制远程工作活动。