GJB

中华人民共和国国家军用标准

FL

GJB 1281—91

指挥自动化计算机网络安全要求

Security requirements of computer networks for command automation

1991—12—23 发布

1992—09—01 实施

国防科学技术工业委员会 批准

目　　次

中华人民共和国国家军用标准

指挥自动化计算机网络安全要求 GJB 1281—91

Security requirements of computer networks for command automation

1 范围

1.1 主题内容和适用范围

1.1.1 本标准规定了全军指挥自动化计算机网络在实体、网络和管理等方面的安全要求(未涉及可靠性安全要求)。可作为论证、招标、研制、验收和应用的基本依据。

其它计算机网络,特别是国家重点要害部门的计算机网络也可参照采用。

1.1.2 本标准适用于指挥自动化广域网和局域网。

2 引用文件

GB 2887 计算站场地技术要求

GB 4943 数据处理设备的安全

GB 9361 计算站场地安全要求

GJB 141.1 用于数据传输的一般专用标准电话电路特性

GJB 141.2 用于数据传输的优质专用标准电话电路特性

GJB 148 数据传输质量维护极限及维护标准

GJB 151 军用设备和分系统电磁发射和敏感度要求

GJB 663 军用通信系统、设备安全要求

3 定义

3.1 信息破坏

由于偶然事故或人为因素而破坏信息的正确性、完整性和可用性。

3.2 网络实体

计算机网络中各类设备(包括节点机设备、通信设备、终端设备、存储设备、电源系统等)以及为此服务的其他硬件设备的总称。

3.3 计算机病毒

依附在计算机程序中的一种可以繁衍的程序。它象生物病毒一样使计算机程序感染,并在计算机网络中再生和扩散,造成其紊乱或瘫痪。

3.4 最小特权

在完成某种操作时所赋予网络中每个主体(用户或进程)必不可少的特权。

国防科学技术工业委员会 1991—12—23 发布 1992—09—01 实施

3.5 **主动威胁**

非法占用网络处理信息、侵入文件、修改程序，造成在错误状态下运行。

3.6 **被动威胁**

当网络正常运行时，由于系统单元暴露或输入输出等管理不严造成信息泄露或被非法截取而产生的威胁。

3.7 **实体安全（物理安全）**

为确保网络在信息的采集、处理、传输、存储过程中，不致受到人为或自然因素的危害，而对网络设备、设施、环境、人员等所采取的安全措施。

3.8 **灾难事件**

因人为或自然灾害造成的涉及全局的一时难以恢复的破坏性事件。

4 一般要求

4.1 目标

网络安全设计应与论证、招标、研制、验收和应用工作同步进行，并根据需求，分阶段、分层次逐步实施和完善，以达到如下目标：

a. 保证网络正常运行，避免各种非故意的错误与损失；

b. 保证信息的正确性、完整性和可用性，防止网络及数据遇到偶然的、被动的和主动的威胁，以及自然灾害的破坏；

c. 对影响网络的意外事件具有应急措施。

4.2 基本原则

4.2.1 特权分散原理

把实现某一重要功能的特权分散给若干个程序、节点或用户，必须由规定的若干个具有特权的程序、节点或用户到齐后才能实现该功能。

4.2.2 最小特权原理

应限定网络中每个主体所必须的最小特权，确保可能的事故、错误、网络部件的篡改等原因造成的损失最小。

4.2.3 安全控制和对象的独立性

安全控制的设计、实现和操作应隔离。

4.2.4 分割和分区化

对网络中受保护的内容分割成几个部分，并分别加以保护。

4.2.5 参数化

安全控制设计应参数化，以便授权时加以调节。

4.2.6 隐蔽

对工作人员和受控对象（用户）隐蔽控制手段及其操作详情。

4.2.7 经济性

对网络中须保密的设备，采用经济有效的控制设计达到要求。所占资源应少于系统资源的10%。

4.2.8 安全形象

全网络在用户和公众面前应具有完整的安全形象。

4.3 基本要求

4.3.1 应具有对全网网络拓扑、网络配置及网络参数的统一管理，监督与控制功能。

4.3.2 对网络实体的环境安全、电磁干扰和辐射的保护应有安全措施。

4.3.3 网络系统应有技术安全手段，确保数据传输、交换、存储处理及通信控制的安全。

4.3.4 网络应具有计算机病毒的预防措施。

4.3.5 对灾难性事件应有应急措施。

4.3.6 网络应具有必要的冗余度和降级处理能力。

4.3.7 网络安全设施的接口设备应方便用户并实现透明操作。

4.3.8 网络应具有承受允许的最严重错误的能力

4.3.9 在确保安全的前提下应充分发挥资源共享的效能。

4.3.10 网络应采取多重安全控制手段。每个安全控制手段均能产生充分的证据，以表明所完成操作的正确性。

4.3.11 网络应登记用户进入网络的各种活动，以提供事后检查。

4.3.12 存取控制应是逐级授权的。网络在为授权用户提供合法服务的同时，应具有拒绝非法访问的功能。

4.3.13 应具有监视和控制网络负载状态的功能，以防止其崩溃和瘫痪。

5 详细要求

5.1 实体安全（物理安全）

威胁实体安全的具体表现如下：

a. 人为破坏；

b. 各种自然灾害；

c. 各类媒体失窃和散失；

d. 设备故障；

e. 环境和场地因素；

f. 电磁发射及敏感度；

g. 战争的破坏等。

5.1.1 网络节点场地环境安全要求

网络节点中心应设专用机房，装备空调、在线式不间断供电电源、报警、防水、防盗、防鼠和消防设备以及电磁防护、接地及避雷装置。

5.1.1.1 设计或改建网络节点机房时必须符合 GB 2887 和 GB 9361 的规定。

5.1.1.2 网络节点机房建筑和结构还应注意下列问题：

a. 宜为专用建筑；

b. 在电梯或楼梯应设置不能直接进入机房的场所；

c. 应与外部人员频繁出入的场所隔离；

d. 周围应设有防止非法进入的设施；

e. 建筑物周围应有足够照度的照明设施；

f. 外部容易接近的窗口应采取防范措施。无人值守时应有自动报警设备；

g. 应只有一个出入口，并在合适的位置上开设应急出入口，作为应急疏散通道。出入口处均应安装出入控制装置；

h. 内部设计应便于出入控制和分区控制。

5.1.1.3 安全设备除符合 GB 9361 规定外，还应满足下列要求：

a. 机房进出口须设置应急电话；

b. 各房间应有声光报警装置；

c. 进出口应派警卫或设置识别与记录进出人员的设备及防范措施；

d. 机房内用于动力、照明的供电线路应与计算机系统的供电线路分开；

e. 机房内不同电压的供电系统应安装互不兼容的插座；

f. 应配备温、湿度自动记录仪及温、湿度报警设备和碎纸机；

g. 机房及疏散通道须配备应急照明装置(5 勒克斯)。

5.1.2 网络终端场地环境安全要求

5.1.2.1 终端室的环境

a. 应具备适当的通风和空调；

b. 应清洁无尘；

c. 应具备防静电措施；

d. 应设置温、湿度计、吸尘器以及碎纸机；

e. 终端宜采取屏蔽措施，如屏蔽罩等；

f. 处理密级数据的远程终端应放置在相应的安全环境中。

5.1.2.2 终端室电源防护应根据需要选用离线式或在线式不间断供电电源。

5.1.2.3 防火、防烟、防水和防鼠害

a. 应设置灭火器，并根据需要安装火灾探测器；

b. 将当地消防队电话号码张贴在电话机附近；

c. 定期检查火灾探测设备或灭火器以及水敏传感器，并保存这类检查的书面报告。

d. 指定并训练人员担任扑灭小火或闷燃火灾的消防员；

e. 终端室严禁吸烟；

f. 禁止使用延伸接线盒和多通电源插座；

g. 机房窗帘使用阻燃材料制作；

h. 应有应急供电的备用照明；

i. 设备不得紧靠墙壁放置；

j. 在设备周围不要堆积大量纸张，以免堵住设备的通风孔；

k. 设备上严禁放置无关物品；

l. 终端室不要有水管、蒸汽管道通过天花板；

m. 如果终端室屋顶有水塔或冷却器，必须采用防护装置；

n. 每台设备应配置防水罩；

o. 在易受鼠害的场所，电缆和电线上应涂驱鼠药剂；

p. 应设置捕鼠和驱鼠装置。

5.1.2.4 防盗

a. 采用特殊门锁；

b. 每个设备都应附有标签或标记；

c. 应设警报器；

d. 可采用锚式锁固定终端设备；

e. 可在终端上加装锁式电源开 ；

f. 如果用户不愿在设备上打孔安装锁或开关，可在靠近终端处安装独立的锁式电源开关。开关的导线应联至电源插座，终端电源线联到开关。

5.1.3 网络通信系统安全要求

5.1.3.1 网络通信系统安全应符合 GJB 663 规定。

5.1.3.2 网络通信系统传输线路的安全应注意下列问题：

a. 传输线路应符合标准。用于数据传输的电话电路特性应符合 GJB 147.1 和 GJB 147.2。定期检查各线段及接点，更换老化变质的电缆；

b. 传输线路应采用屏蔽电缆并有露天保护或埋于地下，要求远离强电线路或强电磁场发射源，以减少由于干扰引起的数据错误；

c. 铺设电缆应采用金属铠装、屏蔽电缆或加装金属套管，以减少各种监控辐射对线路的干扰；

d. 加装中和变压器、屏蔽变压器和绝缘变压器；

e. 宜采用光纤电缆；

f. 定期测试信号强度，检查是否有非法装置接入线路；

g. 定期检查接线盒及其它易被人接近的线路部位；

h. 调制解调器应放置在受监视的区域，以防止外来连接的企图。调制解调器的连接应定期检验，以检验是否有篡改行为。

5.1.4 电磁兼容和防护

5.1.4.1 网络设备的电磁兼容，按 GJB 151 有关规定限值选用。

5.1.4.2 要防止电磁辐射被截收。

a. 入网设备必须符合 GJB 151 规定；

b. 重要场合应对机房进行屏蔽；

c. 可采取区域控制的办法；

d. 采取主动有源干扰等技术；

e. 机房宜设在地下室或底层。

5.1.4.3 网络通信系统必须具有防止电磁干扰和泄漏的措施。

5.1.5 记录媒体的保护

5.1.5.1 载有关键性程序、主记录、设备分配图表、加密算法、密钥等记录媒体应按其密级及

其产生的难易程度分级管理和保护。

5.1.5.2 载有关键记录的磁盘、磁带等磁媒体应加防磁场保护措施，必要时需进行备份保护。

5.2 网络系统安全

5.2.1 信息传输安全

a. 密级信息到达终点之前，严禁呈现明文状态；

b. 传输密级信息时必须进行网络加密，如链路加密、节点加密和用户加密等；

c. 为保证密级数据的安全传递，网络节点机宜有备份；

d. 不传送信息时接口应阻断；

e. 设置辨认正当通信伙伴的功能；

f. 用拨号线能接触网络时，拨号码应予以保护。同时保密信息不宜存放在节点机内。

5.2.2 鉴别

5.2.2.1 为了防止非法修改节点机中的通行字表，应具备鉴别用户通行字真实性的能力；

5.2.2.2 对用户密钥应鉴别；

5.2.2.3 在数据通信中，应有验证接收到的数据是否真实的能力；

5.2.2.4 应能识别非法入网的终端和用户。遇有多次不成功的联机尝试时，应及时记录并分析结果，采取相应的处理。

5.2.3 输入输出控制

5.2.3.1 明确网络系统各环节工作人员的职责

a. 设计人员与操作人员必须分离；

b. 重要事务处理项目，必须由法定人办理；

c. 工作期间至少应有二人在场，以防止非法使用网络；

d. 必须保存控制台打印记录。

5.2.3.2 制订统一的数据格式并使用标准编码。

5.2.3.3 操作控制

a. 对特定的终端设备，应采用通行字、卡片、识别码、钥匙等办法限定操作人员。

b. 操作人员操作应符合有关操作规程和输入/输出数据处理的规定；

c. 应建立良好的人机操作环境，以减少失误；

d. 处理密级数据的各终端应予隔离。

5.2.3.4 数据在投入使用前，必须确保其准确可靠。

5.2.3.5 输出控制

a. 各业务部门终端数据输出控制应有专人负责；

b. 输出文件必须有明显的、可读的密级标志；

c. 输出文件的发放应按规定生成所申请数量的拷贝。网上传输文件，收方应给回执；

d. 打印过保密数据的色带，应妥善保管或销毁。

5.2.3.6 内存的残留信息应及时清除，以防止引起信息泄漏。

5.2.3.7 设备无人值守运行时，应切实地对运行状态进行监视、控制及记录。如运行状态的监视、运行控制、记录运行状态。

5.2.3.8 在互通的计算机系统之间，建立能检查判断对方是否正常工作的功能。

5.2.3.9 应具有检测不正当使用和非法存取的监视(记录)功能。如存取监视功能、控制台记录功能、系统使用状况记录功能等。

5.2.3.10 对不设在专用机房的计算机，应采取下列措施以预防程序及数据不正当使用和更改。

a. 下线的计算机不应保存重要的程序及数据文件；

b. 上线时应对重要程序及数据文件进行必要的检测，以避免不正当更改；

c. 对上线计算机应设置监视功能，以对不正当输入及事件进行检查。

5.2.4 联网处理

联网时不得影响互联双方原有的安全性。

5.2.5 密码保护

5.2.5.1 密码算法的设计、研制、投入使用必须报请密码主管部门批准，并由指定的密码研制单位研制生产。

5.2.5.2 网络应根据划分的密级处理相应的信息。密码算法的保密强度必须与被保护信息的密级相适应，严禁在低密级环境中处理、传输、存储高密级信息。

5.2.5.3 网络的关键程序、密码算法、密钥等软件数据，必须受到保密保护或其它形式的有效保护。

5.2.5.4 用于链路加密、节点加密、终端加密的算法要相互分割。

5.2.5.5 不同系统间的密码体制既要相互分割，又要能保证系统间通信。

5.2.5.6 在紧急情况下，密钥受到意外破坏时的恢复等问题，要有妥善可行的应急措施。

5.3 计算机病毒的预防

5.3.1 不要用非发行包软盘引导系统。

5.3.2 基于软盘的计算机，应使用确认无病毒的磁盘启动系统，该盘应贴上作为系统引导盘的标签。

5.3.3 基于硬盘的计算机应尽可能的避免由软盘引导。

5.3.4 谨慎使用公共软件和共享软件。公用和共享软件切勿放在根目录中。

5.3.5 格式化时为所有硬、软盘建立卷标，且在每次执行目录命令时检查卷标，注意卷标的任何变化。

5.3.6 监视系统运行方式的变化，记录并分析异常现象。

5.3.7 系统之间应尽可能地减少可执行代码的交换。

5.3.8 所有的引导软盘均应是写保护的。对某些高保安环境，应使用硬盘写保护系统。

5.3.9 当软盘片不经常使用时，应从驱动器中取出，并作为文件归档。

5.3.10 禁止在联网计算机上运行任何游戏盘。

5.3.11 禁止使用非本单位软盘。重要部门要使用专机、专盘。

5.3.12 非本机使用的软盘或新开发的软件，须经检测，确认没有病毒方可在系统上使用。

5.3.13 本机使用的软盘不得外借或使用者随意携带外出。

5.3.14 系统中的数据要定期拷贝。

5.3.15 网络中所用记录媒体应经常进行病毒检测，当发现病毒时，应立即采取隔离措施，防止病毒在网上扩散，并设法消除之。

5.3.16 宜采取信号抗病毒措施，防止病毒依附着无线电信号进入接收机、处理机；

5.3.17 购置、引进设备或将设备送外维修，要考虑对病毒的防范 如将设备进行全部"清洗"，并运行一段时间后再上网。

5.4 局域网的安全

除应符合本标准第4章、第5章上述要求外，还应符合以下要求。

5.4.1 识别与认证

网络必须具有准确地识别终端用户的功能。所采用的通行字必须有加密措施。

5.4.2 随机存取控制

5.4.2.1 局网上的信息应采取保护措施(如采用防穿刺电缆等)，以防"监听"。

5.4.2.2 应在每个受保护的文件上标明存取权限，并对其进行保护。

5.4.3 所有存储目标(RAM，磁盘段)在使用后，应回到"原始"状态。不应附有任何其它信息。

5.4.4 不论用户在工作站或服务器上处理数据，系统应具 跟踪记录用户作业过程、违例行为以及驱动器和目录的变化能力，并用二进制加密文件存储检查追踪，此文件只允许保密人员或指定人员使用。

5.5 灾难性事件应急处理要求

5.5.1 制定紧急行动方案和明确各种措施的负责人。

5.5.2 原计算机进行的工作，及时转入以下可行的替代方式：

a. 手工进行；

b. 由部分设备继续进行或转移到其它的计算机系统上进行；

c. 暂时停止处理。

5.5.3 应有尽快恢复网络正常运行所需的相应措施。

5.6 安全管理

5.6.1 网络管理

5.6.1.1 按本标准4.3.1的规定执行。

5.6.1.2 对网络系统的规模、组成、结构、功能、数据类型、业务特点、使用环境和用户性质进行分类，使业务部门与相应的数据对应，工作性质与功能对应。

5.6.1.3 明确划分不同用户的存取权限，并由专人存取和修改授权表。

5.6.1.4 值班负责人要每天审阅并处理与网络安全有关的记录。

5.6.1.5 定期检查网络中有无造成信息泄露的迹象。

5.6.2 设备管理

5.6.2.1 入网的硬件设备应符合统一规定的型号和标准，并且是经过安全认证和EMC认证的产品。

5.6.2.2 必须定期进行安全设施使用及维护训练，保证有关人员能熟练地操作。

5.6.2.3 重要的网络节点、终端及外设应配置备用设备。

5.6.2.4 通信线路应按标准维护。用于数据传输的电话电路特性及维护按GJB 147.1、GJB

147.2 和 GJB 148 规定执行。

5.6.2.5 密码机的使用安全管理按全军《密码机使用规范》规定执行

5.6.2.6 网络使用过程中，应有专人负责密钥管理工作。密钥的管理、使用方法和措施，如产生、保管、配发、更换、销毁等，按全军《密钥管理规定》执行。

5.6.3 人员管理

5.6.3.1 人员审查

必须根据网络业务所定的密级确定人员审查标准。处理机要信息的人员应按机要人员的标准进行审查。

5.6.3.2 关键岗位的人选

对网络和各节点系统管理员要有严格的政审以及现实表现、工作态度、道德修养和业务能力等方面的考察。

5.6.3.3 网络全体人员须经安全培训后方能上岗工作。

5.6.3.4 对网上全体人员应定期进行考核，不适合接触系统的人员应及时调离。

5.6.3.5 对调离人员，要其承担调离后的保密义务。立即收回所有钥匙及证件，退还全部技术手册和有关材料。系统必须立即更换通行字和机要锁。

5.6.4 建立健全各种管理制度

a. 网络节点中心和用户终端室管理；

b. 网络执勤维护管理；

c. 文件管理；

d. 信息媒体管理；

e. 文电收发管理；

f. 计算机病毒预防；

g. 机房清洁管理；

h. 危险品管理；

i. 消耗品管理；

j. 机房有关安全保密管理；

k. 节点机及终端操作规程；

l. 数据及程序的保管管理；

m. 电源、空调设备，防灾、防范设备管理；

n. 监察体制及监视的规章制度。

附加说明：

本标准由总参通信部提出。

本标准由海军装备论证研究中心自动化所、海司通信部负责起草。

本标准主要起草人：李熙玉、李忠国、李九重、石延岭、寇国华、李树人、王利剑、周凤武。