# 2024年全国“两会”期间网络与信息安全信息通报工作通知

来源：网络 作者：无殇蝶舞 更新时间：2025-04-25

*第一篇：2024年全国“两会”期间网络与信息安全信息通报工作通知各区（县、市）统计局：根据《浙江省统计局办公室关于做好2024年全国“两会”期间网络与信息安全信息通报工作的通知》（x统办函[2024]x号）的要求，现将“两会”期间网络与信...*

**第一篇：2024年全国“两会”期间网络与信息安全信息通报工作通知**

各区（县、市）统计局：

根据《浙江省统计局办公室关于做好2024年全国“两会”期间网络与信息安全信息通报工作的通知》（x统办函[2024]x号）的要求，现将“两会”期间网络与信息安全信息通报工作有关事项通知如下：

一、切实加强通报工作的组织部署

“两会”期间的信息通报专项工作自3月3日开始至16日结束。各区（县、市）要充分认识做好“两会”期间信息通报工作的重要性，切实增强政治责任感、大局意识，强化底线思维，克服麻痹思想，切实加强对本单位网络安全防范和信息通报工作的组织领导，严格落实各项要求，确保制度到位，人员到位，措施到位。

各地要及时收集、研判和通报网络与信息安全的情况信息及重大安全事件，提高信息安全防范和应急响应能力，确保“两会”期间统计信息系统安全运行。

二、加强重要信息系统和网站安全隐患检查整改

（一）各区（县、市）应对本单位的网站和重要信息系统进行全面安全检测，对发现的问题和隐患要第一时间整改，受技术条件限制不能立即整改到位的，必须制定可操作的应对方案，加固防护措施，确保“两会”期间安全。

（二）各区（县、市）应对本单位的终端计算机安装市局统一部署的客户端安全防护管理系统，并及时更新系统补丁，同时要求职工在下班离开办公室前务必关闭终端计算机。

三、做好网络安全应急响应准备工作

各区（县、市）要部署开展对重要信息系统和网站安全状况24小时实时监测，按照网络与信息安全应急预案，做好“两会”期间网络安全应急响应准备和保障工作，确保发生网络安全事件时能妥善快速处置。要加强重要信息系统的值班值守，合理安排人员，保持通讯联络畅通，确保应急处置准确及时。

四、做好网络与信息安全通报工作

“两会”期间，各区（县、市）要于每日14:30时之前完成“日调查表”的填报并上报至市局ftp数据中心目录中。

为能够及时建立工作联系，请各区（县、市）在首次上报“日调查表”时同时上报本单位的基本信息和具体人员的联络信息等内容。

五、联系人及联系方式

联系人：俞xx

**第二篇：网络与信息安全**

《网络与信息安全》复习资料

信息安全特征：完整性、保密性、可用性、不可否认性、可控性。保密学是研究信息系统安全保密的科学。

网络信息安全体系结构框架：安全控制单元、安全服务层面、协议层次。公钥密码：由两个密码组成，每个用户拥有一对选择密钥：加密密钥与解密密钥。公钥密码特点：（1）加密密钥和解密密钥在本质上是不同的，即使知道一个密钥，也不存在可以轻易地推导出另一个密钥的有效算法。（2）不需要增加分发密钥的额外信道。公布公钥空间，不影响公钥系统的保密性，因为保密的仅是解密密钥。公钥密码系统应具备两个条件：（1）加密和解密交换必须满足在计算上是容易的。（2）密码分析必须满足在计算机上是困难的。协议：两个或两个以上的主体为完成某一特定任务共同发起的某种协约或采取的一系列步骤。协议的特征：（1）至始至终有序进行。（2）协议成立至少要有两个主体。（3）协议执行要通过实体操作来实现。数字签名与手写签名的区别：（1）签名实体对象不同。（2）认证方式不同。（3）拷贝形式不同。

签名算法的三个条件：（1）签名者事后不能否认自己的签名。（2）任何其他人都不能伪造签名，接收者能验证签名。（3）当签名双方发生争执时，可由公正的第三方通过验证辨别真伪。

不可否认数字签名：没有签名者的合作，接收者就无法验证签名，某种程度上保护了签名者的利益，从而可防止复制或散布签名文件的滥用。

不可否认数字签名方案由三部分组成：数字签名算法、验证协议、否认协议。

散列函数：一种将任意长度的消息压缩为某一固定长度的消息摘要的函数。消息认证码：满足某种安全性质带有密钥功能的单向散列函数。身份证明分两大娄：身份证实、身份识别。信息隐藏：把一个有含义的信息隐藏在另一个载体信息中得到隐密载体的一种新型加密方式。

信息隐藏的两种主要技术：信息隐秘术、数字水印术。数字水印技术：指用信号处理的方法在数字化的多媒体数据中嵌入隐藏标识的技术。

三种数字水印：（1）稳健的不可见的水印。（2）不稳健的不可见的水印。（3）可见的水印。

数字水印三个特征：（1）稳健性。（2）不可感知性。（3）安全可靠性。

数字水印三个部分：（1）水印生成。（2）水印嵌入。（3）水印提取（检测）。

密钥管理的基本原则：（1）脱离密码设备的密钥数据应绝对保密。（2）密码设备内部的密钥数据绝对不外泄。（3）密钥使命完成，应彻底销毁、更换。常用密钥种类：（1）工作密钥。（2）会话密钥。（3）密钥加密密钥。（4）主机主密钥。

公开密钥分发：（1）广播式密钥分发。（2）目录式密钥分发。（3）公开密钥机构分发。（4）公开密钥证书分发。密钥保护方法：（1）终端密钥保护。（2）主机密钥保护。（3）密钥分级保护管理。

秘密共享方案：将一个密钥K分成n个共享密钥K1、K2……Kn，并秘密分配给n个对象保管。密钥托管技术：为用户提供更好的安全通信方式，同时允许授权者为了国家等安全利益，监听某些通信和解密有关密文。密钥托管加密体制由三部分组成：用户安全分量、密钥托管分量、数据恢复分量。密钥管理：指对于网络中信息加密所需要的各种密钥在产生、分配、注入、存储、传送及使用过程中的技术和管理体制。

保密通信的基本要求：保密性、实时性、可用性、可控性。密码保护技术：密码校验、数字签名、公证消息。通信保密技术：（1）语音保密通信（模拟置乱技术、数字加密技术）。（2）数据保密通信。（3）图像保密通信（模拟置乱、数字化图象信号加密）。网络通信加密的形式：（1）链路加密。（2）端－端加密。（3）混合加密。网络通信访问基本控制方式：（1）连接访问控制。（2）网络数据访问控制。（3）访问控制转发。（4）自主访问控制与强制访问控制。接入控制功能：（1）阻止非法用户进入系统。（2）允许合法用户进入系统。（3）使合法用户按其权限进行活动。接入控制策略：（1）最小权限策略。（2）最小泄漏策略。（3）多级安全策略。接入控制技术方法：（1）用户标识与认证。（2）身份认证特征（口令认证方式、协议验证身份）。

PGP的五种功能：认证性、机密性、压缩、Email兼容性、分段与重组。IP层安全功能：鉴别服务、机密性、密钥管理。

安全套接层SSL提供的安全服务：信息保密、信息完整性、相互认证。

PPDR－A模型五要素：安全策略、安全监测、安全反应、安全防御、安全对抗。操作系统安全访问控制：测试程序访问控制、操作系统的访问权限控制、保护机制的访问控制、用户认证访问控制。

安全操作系统设计四环节：安全模型、安全设计、安全确认、正确实施。安全网络平台种类：Windows NT、UNIX、Linux。（Linux兼容性好、源代码开放、安全透明）。

数据库安全条件：数据独立性、数据安全性、数据完整性、数据使用性、备份与恢复。

VPN（虚拟专用网）核心技术：隧道技术、密码技术、管理技术。

政务网的特点：信息公众化、信息机关化、信息存储量大、保密程度高、访问密级多样化。

政务网建设的三个安全域：（1）涉密域。（2）非涉密域。（3）公共服务域。

黑客攻击：指黑客利用系统漏洞和非常规手段，进行非授权的访问行为和非法运行系统或非法操作数据。

防黑客攻击几种防范技术：安全性设计保护、先进的认证技术、扫描检测审计技术。

常规网络扫描工具：SATAN扫描工具、Nessus安全扫描器、nmap扫描器、strobe扫描器。网络监听工具：NetXRay、Sniffit。防火墙：在网络安全边界控制中，用来阻止从外网想进入给定网络的非法访问对象的安全设备。包括网络级包过滤防火墙和应用级代理防火墙。

密罐：用来观察黑客如何入侵计算机网络系统的一个软件“陷阱”，通常称为诱骗系统。

计算机病毒：指编制或者在计算机程序中插入的破坏计算机功能或者数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。病毒检测方法：比较法、搜索法、辨别法、分析法。

电子商务安全要求：可靠性、真实性、机密性、完整性、有效性、不可抵赖性、可控性。

电子商务安全服务：鉴别服务、访问控制服务、机密性服务、不可否认服务。电子商务基本密码协议：密钥安全协议、认证安全协议、认证的密钥安全协议。国际通用电子商务安全协议：SSL安全协议、SET安全协议、S－HTTP安全协议、STT安全协议。

电子商务实体要素：持卡人、发卡机构、商家、银行、支付网关、认证机构。

**第三篇：2024全国两会信息汇总**

2024全国两会特稿汇总2024全国两会特稿：盘点2024两会“十个热词” 2024全国两会特稿：两会授权发布:当局工作报告 2024全国两会特稿：习近平“中国梦”讲话全文 2024全国两会特稿：李克强总理等会见采访两会的中外记者并回答提问 2024全国两会特稿：李克强总理记者会精彩语录 2024全国两会特稿：国务院组成部门 2024全国两会特稿：机构调整传递光显旌旗灯号：职能变化是最大核心 2024全国两会特稿：国务院将从六个方面变化职能 2024全国两会特稿：两会新华视点：职能变化 新一轮机构改革“大幕”开启 2024全国两会特稿：新华社评论员:赓续深化行政改革,切实变化当局职能 2024全国两会特稿：大部制改革没有“完成时” 2024全国两会特稿：治污先治官，须完美考核和问责 2024全国两会特稿：品读李总理“以民之所望为施政所向” 2024全国两会特稿：人民日报评论员：建设服务型当局的新突破 2024全国两会特稿：人民日报评论员：以绿色发展构建鲜艳中国——五论以实干贯彻十八大精神 2024全国两会特稿：人民日报人民时评：让更多人共享人生出彩的机会 2024全国两会特稿 ：成就奋发人心 梦想凝聚力量——海外华侨华人畅谈中国梦 2024全国两会特稿：人民日报今日谈：新型城镇化深圳回收礼品浙江人事考试中心企业邮箱搜索引擎优化，关键是质量 2024全国两会特稿：总理答记者问解读：有感于李克强总理的实现三项义务必要三大保障 2024全国两会特稿：中国梦的新起点 2024全国两会特稿：习近平提“人民共同享有人生出彩的机会”鼓舞人心 2024全国两会特稿：城镇化“三问”——人大代表谈如何破解“三农”发展难题 2024全国两会特稿：昂扬奋进的接续时刻——新任国务院总理产生侧记 2024全国两会特稿：“新四化”同步 共圆小康梦 2024全国两会特稿：新起点·新使命·新期盼——写在国务院机构改革和职能变化方案通过之际 2024全国两会特稿：李立国回应“人猪穿越答问”：猪不存在火化题目 2024全国两会特稿：新华网专访黄奇帆：推动伶俐型“山城特色”改革 2024全国两会特稿：代表委员建言:严控“三公消耗” 既要盯“钱”更要管“权” 2024全国两会特稿：中国梦”的世界对话 2024全国两会特稿：反映最原汁原味的民意--农夫工代表集体“发声”为草根代言 2024全国两会特稿：启航时刻——全国政协十二届一次会议推举侧记 2024全国两会特稿：红地皮的绿色崛起之梦——访江西省省长鹿心社 2024全国两会特稿：代表委员聚焦互联网行业三大乱象：能否还一片净土？ 2024全国两会特稿：“房腐证腐号腐”,腐腐该惩--代表委员拷问新型腐败 2024全国两会特稿：代表委员热议新一轮机构改革和职能变化 2024全国两会特稿：依法治国的司法实践--从两高报告透视五年司法建设之路 2024全国两会特稿：更安心·更便利·更诚信——国务院机构改革和职能变化方案透出“三大民生指向” 2024全国两会特稿：两会聚焦下层 放飞民生梦想 2024全国两会特稿：提案背后是担当--农工民主党中间治理灰霾提案追踪 2024全国两会特稿：“新”在哪里 “化”在何方——代表委员三论“新型城镇化” 2024全国两会特稿：中国特色社会主义事业站在了新的历史起点上--吴邦国代表全国人大常委会作工作报告 2024全国两会特稿：代表委员呼吁用制度监管束缚“三公经费” 2024全国两会特稿：“农海归”、农二代、留守儿童--代表委员热议“人的城镇化”三大重点人群 2024全国两会特稿：从报告看当局自身建设路径 2024全国两会特稿：中国将合理控制特大城市规模追求城镇化科学发展 2024全国两会特稿：怎么分,才合理?--代表委员“支招”收入分配改革 2024全国两会特稿：民生增支和百姓增收：“两条曲线”折射中国民生美好图景 2024全国两会特稿：从土生土长到“道行天下”--道教正向国际性宗教发展 2024全国两会特稿：当局工作报告中的民生路径 2024全国两会特稿：用制度的笼子“关住”腐败——代表委员纵议制度反腐 2024全国两会特稿：跨越再跨越——十一届全国政协走过五年 2024全国两会特稿：向着绚丽的“中国梦”,进发--写在2024年“两会时刻”开启之际 2024全国两会特稿：慈善之殇将撬动中国

社会福利事业变革 2024全国两会特稿：八成省份GDP目标增速超10% 资源、环境hold得住吗? 2024全国两会特稿：生态灾祸成“天下第一难” 谁是“带毒GDP”背后推手? 2024全国两会特稿：如何让百姓对内地奶粉重拾信赖?——香港限粉令引热议 2024全国两会特稿：肩负人民信赖 传达百姓心声——十二届全国人大一次会议京外代表团抵京侧记 2024全国两会特稿：两会倒计时：十二届全国人大一次会议看点导读 2024全国两会特稿：“草根”代表路 “最美”中国梦 2024全国两会特稿：中国将与世界共逐“和平发展”梦 2024全国两会特稿：从十八大到全国两会：吹响实现“中国梦”的时代号角 2024全国两会特稿：“同票同权”后的全国人大代表首次登上国家政治舞台 2024全国两会特稿：政协委员建议：遏制餐桌虚耗先向公款吃喝“开刀” 2024全国两会特稿：政协委员“三问”另一种虚耗 2024全国两会特稿：全球视野下的两会期待——2024年两会热点前瞻 2024全国两会特稿：同心同向的时代步伐——人民政协五年亮点扫描 2024全国两会特稿：人人平等、地区平等、民族平等——十二届全国人大代表构成特色分析 2024全国两会特稿：肩负起人民的重托——十二届全国人大代表构成特色分析 2024全国两会特稿：修建实现“中国梦”的坚实支持——欢迎两会述评之三

**第四篇：证券期货业网络与信息安全信息通报暂行办法**

证券期货业网络与信息安全信息通报暂行办法

2024年07月20日 16:00 来源： 金融界网站 【字体：大 中 小】 网友评论

（2024年2月1日 证监信息字〔2024〕1号）

第一条为规范证券期货行业网络与信息安全信息通报工作，切实保护投资者合法权益，依据国家有关规定，制定本办法。

第二条证券期货行业信息安全保障协调小组（以下简称协调小组）负责行业网络与信息安全信息通报工作的决策、组织、协调工作，协调小组成员单位包括中国证监会、上海证券交易所、深圳证券交易所、上海期货交易所、大连商品交易所、郑州商品交易所、中国证券登记结算公司、中国证券业协会和中国期货业协会。信息通报单位包括证券、期货交易所，中国证券登记结算公司，各证券公司、基金管理公司、期货公司，证券、期货投资咨询公司以及其他由证监会核准注册成立的机构（以下简称通报单位）.第三条中国证监会信息中心是协调小组的执行部门，负责向国家网络与信息安全信息通报中心报告证券期货行业的网络信息安全信息;负责将国家网络与信息安全信息通报中心发布的信息报告、病毒与网络攻击预警等按要求向协调小组单位成员传达，并通过中国证券业协会和中国期货业协会向各自归口的通报单位传达。

中国证监会信息中心作为协调小组中各通报单位的归口单位，负责这些单位网络与信息安全信息的汇总、整理。

中国证券业协会负责证券公司、基金管理公司、证券投资咨询公司等单位的网络与信息安全信息汇总和反馈工作，并作为上述机构的归口单位向中国证监会信息中心报告。

中国期货业协会负责期货公司、期货投资咨询公司等单位的网络与信息安全信息汇总和反馈工作，并作为上述机构的归口单位向中国证监会信息中心报告。

第四条各通报单位按照“谁主管、谁负责，谁运营、谁负责”的原则，做好各自单位的信息安全通报工作。各单位信息安全工作的责任人（主管领导）为本单位信息安全通报工作的责任人。

各通报单位应落实承担网络与信息安全信息通报工作的职能部门、负责人和联络员，制定本单位内部的信息报告流程和相应的责任制，并填写信息安全报告基本情况备案表（见附件一）报归口单位备案。

各通报单位要及时将本单位网络与信息系统出现的安全事故上报归口单位，并负责将来自归口单位的信息安全通告以及其他通知、要求及时传达到有关责任人。

第五条各通报单位实行7×24小时联络制度，指定一名联络员，一名后备联络员。联络员和后备联络员应有及时准确的通讯联络方式；联络方式如有变动，应填写基本情况变动更新表（见附件一）及时报告归口单位。归口单位要及时维护和更新联络通信录，并在通报体系中公告。

第六条事故报告。通报单位的重要网络与信息系统在运行中出现异常情况，造成不良影响或损失的，应按照应急预案及时处置，同时应将事故发生的情况、危害程度、处置措施、分析研判等内容编写成事故报告，及时上报归口单位（事故分级、报告要素及要求见附件二及编制说明）.第七条信息安全运行月报。为及时反映行业信息安全状况，保持行业信息安全通报系统的畅通，各通报单位每月应以信息安全运行月报（格式见附件三）的形式向归口单位报告信息系统运行情况。

信息安全运行月报的内容为各通报单位信息系统运行中出现并得到及时处置的异常情况汇总和分析、研判，无异常情况的，要进行平安运行报告。对已按事故报告要求上报的情况，要在运行月报中说明。

各通报单位应在每个月前5个工作日内将上个月的系统运行情况上报归口单位。

第八条敏感时期报告。中国证监会信息中心根据国家有关规定和需要启动敏感时期报告制度，并规定行业内敏感时期报告的启动与截止日期、日报告的截止时间等要素。

各通报单位在收到启动敏感时期报告的通知以后，根据要求每日以敏感时期信息安全报告（见附件四）的形式上报本单位信息系统运行状况。报告内容包括信息安全运行月报、事故报告应报的范围。无异常情况的，要进行平安运行报告。

各通报单位在敏感时期应有专人值守。

第九条信息安全通告。中国证监会信息中心、中国证券业协会、中国期货业协会等信息通报归口单位，通过信息通报体系，向各通报单位定期或不定期地发布下列信息安全通告：

国家网络与信息安全信息通报中心发布的报告和预警；

行业信息安全月报的汇总分析；

行业信息系统运行中带有普遍性的安全隐患或趋势；

有关信息安全的通知、规定、技术标准、指引等；

其他需要及时向报告单位通报的信息。

各通报单位在收到归口单位的信息安全通告后，应及时传达到相关责任人，采取相应措施。

第十条各通报单位应切实保证信息通报和联络渠道的畅通。敏感时期报告和信息安全运行月报可使用电子文件的形式报送。对于事故报告，应同时使用书面和电子文件的形式进行报送。对于有保密要求的，应使用符合要求的加密设备进行报送。

第十一条各通报单位应保证上报要素完备、及时、准确，不得瞒报、缓报、谎报网络与信息安全事件的情况。接报单位应保证及时接收、准确记录上报信息。

第十二条各单位应制定相应的保密和档案管理措施，妥善管理上报材料，包括各单位进行信息安全通报过程中往来电话记录（手机或固定电话）、纸质或电子文件、传真件等，存档备查。

第十三条对于认真履行本办法，及时报告网络与信息安全事故的单位及个人，予以通报表扬。对违反本办法及相关制度的单位及个人，予以通报批评；情节严重的，予以行政处分。

第十四条本办法自发布之日起实施。本办法由中国证监会负责解释。

附件一：信息安全报告基本情况备案、变动更新表

附件二：证券期货业网络与信息安全事故报告

附件三：证券期货业网络与信息系统安全运行月报

附件四：证券期货业网络与信息系统敏感时期安全情况日报

附件一：信息安全报告基本情况备案、变动更新表

附件二：证券期货业网络与信息安全事故报告

附件二填制说明：

事故标准及报告要求

重要业务系统出现异常，系统恢复时间（RTO-Recovery Time Objective）在30分钟以内；

因病毒、攻击、拥堵等使系统异常，给市场或客户造成可感知的影响，但交易时段2个小时内恢复的；

系统数据完整性被破坏，但在1个交易日内能够修复的；

灾害事故（停电、水灾、火灾等）发生后，重要业务系统能在1个交易日恢复正常；

网站上出现有害信息，但能及时删除、屏蔽并保留审计线索的；

通信线路发生故障且对业务造成不良影响，1个交易日内系统恢复正常；

敏感业务数据泄漏。

各通报单位的重要信息系统，凡是出现上述情况，都要在2天内，将事故发生的情况、处置措施、影响分析，以事故报告的形式，及时上报归口单位。

重大事故标准及报告要求

各信息报告单位重要信息系统出现重大故障，已经（或预计将）造成重大损失（100万元以上），或给客户/市场带来重大不良影响的。包括但不限于：

重要业务系统出现异常，系统恢复时间（RTO-Recovery Time Objective）在30分钟以上；

因病毒、攻击、拥堵等使系统异常，给市场或客户造成可感知的影响，且交易时段2个小时内没有恢复；

业务数据完整性被破坏，且在1个交易日内没有修复；

通信线路发生故障，对业务造成严重影响，且在1个交易日系统没有恢复正常；

灾害事故（停电、水灾、火灾等）发生后，重要业务系统在一个交易日系统没有恢复正常；

网站上出现有害信息，且未能及时删除、屏蔽或未能保留审计线索的。

各通报单位的重要信息系统，凡是出现上述情况，都要在事故确认的当日（或6小时之内），将事故发生的情况、影响分析、目前的状况、已经采取的处置措施等，以重大事故报告的形式，上报归口单位。

其中，交易、通信、清算等带有全局性的重大系统故障，在及时启动应急预案的同时，还要在2小时内将事故情况上报中国证监会信息中心。

灾难事故标准及报告要求

因自然灾难、人为故意破坏以及其他意外因素，使本单位重要业务系统不能正常运行，并造成恶劣影响或严重损失的，预计有效处置或消除其不良影响需要动员大量社会资源的，应在事故发生后，立即上报归口单位。

附件三：证券期货业网络与信息系统安全运行月报

附件四：证券期货业网络与信息系统敏感时期安全情况日报

**第五篇：网络信息安全**

网络信息安全

信息安全是指为建立信息处理系统而采取的技术上和管理上的安全保护，以实现电子信息的保密性、完整性、可用性和可控性。当今信息时代，计算机网络已经成为一种不可缺少的信息交换工具。然而，由于计算机网络具有开放性、互联性、连接方式的多样性及终端分布的不均匀性，再加上本身存在的技术弱点和人为的疏忽，致使网络易受计算机病毒、黑客或恶意软件的侵害。面对侵袭网络安全的种种威胁，必须考虑信息的安全这个至关重要的问题。

网络信息安全分为网络安全和信息安全两个层面。网络安全包括系统安全，即硬件平台、操作系统、应用软件;运行服务安全，即保证服务的连续性、高效率。信息安全则主要是指数据安全，包括数据加密、备份、程序等。

1．硬件安全。即网络硬件和存储媒体的安全。要保护这些硬设施不受损害，能够正常工作。

2.软件安全。即计算机及其网络中各种软件不被篡改或破坏，不被非法操作或误操作，功能不会失效，不被非法复制。

3.运行服务安全。即网络中的各个信息系统能够正常运行并能正常地通过网络交流信息。通过对网络系统中的各种设备运行状况的监测，发现不安全因素能及时报警并采取措施改变不安全状态，保障网络系统正常运行。

4.数据安全。即网络中存储及流通数据的女全。要保护网络中的数据不被篡改、非法增删、复制、解密、显示、使用等。它是保障网络安全最根本的目的。

1.防火墙技术。防火墙（Firewall）是近年来发展的最重要的安全技术，它的主要功能是加强网络之间的访问控制，防止外部网络用户以非法手段通过外部网络进入内部网络（被保护网络）。它对两个或多个网络之间传输的数据包和链接方式按照一定的安全策略对其进行检查，来决定网络之间的通信是否被允许，并监视网络运行状态。简单防火墙技术可以在路由器上实现，而专用防火墙提供更加可靠的网络安全控制方法。

防火墙的安全策略有两条。一是“凡是未被准许的就是禁止的”。防火墙先是封闭所有信息流，然后审查要求通过的信息，符合条件的就让通过；二是“凡是未被禁止的就是允许的”，防火墙先是转发所有的信息，然后再逐项剔除有害的内容，被禁止的内容越多，防火墙的作用就越大。网络是动态发展的，安全策略的制定不应建立在静态的基础之上。在制定防火墙安全规则时，应符合“可适应性的安全管理”模型的原则，即：安全=风险分析+执行策略+系统实施+漏洞监测+实时响应。防火墙技术主要有以下三类：

●包过滤技术（Packct Filtering）。它一般用在网络层，主要根据防火墙系统所收到的每个数据包的源IP地址、目的IP地址、TCP/UDP源端口号、TCP/UDP目的端口号及数据包中的各种标志位来进行判定，根据系统设定的安全策略来决定是否让数据包通过，其核心就是安全策略，即过滤算法的设计。

●代理（Proxy）服务技术。它用来提供应用层服务的控制，起到外部网络向内部网络申请服务时的中间转接作用。内部网络只接受代理提出的服务请求，拒绝外部网络其它节点的直接请求。运行代理服务的主机被称为应用机关。代理服务还可以用于实施较强的数据流监控、过滤、记录等功能。

●状态监控（Statc Innspection）技术。它是一种新的防火墙技术。在网络层完成所有必要的防火墙功能——包过滤与网络服务代理。目前最有效的实现方法是采用 Check Point）提出的虚拟机方式（Inspect Virtual Machine）。

防火墙技术的优点很多，一是通过过滤不安全的服务，极大地提高网络安全和减少子网中主机的风险；二是可以提供对系统的访问控制；三是可以阻击攻击者获取攻击网络系统的有用信息；四是防火墙还可以记录与统计通过它的网络通信，提供关于网络使用的统计数据，根据统计数据来判断可能的攻击和探测；五是防火墙提供制定与执行网络安全策略的手段，它可以对企业内部网实现集中的安全管理。

防火墙技术的不足有三。一是防火墙不能防止绕过防火墙的攻击；二是防火墙经不起人为因素的攻击。由于防火墙对网络安全实施单点控制，因此可能受到黑客的攻击；三是防火墙不能保证数据的秘密性，不能对数据进行鉴别，也不能保证网络不受病毒的攻击。

2.加密技术。数据加密被认为是最可靠的安全保障形式，它可以从根本上满足信息完整性的要求，是一种主动安全防范策略。数据加密就是按照确定的密码算法将敏感的明文数据变换成难以识别的密文数据。通过使用不同的密钥，可用同一加密算法，将同一明文加密成不同的密文。当需要时可使用密钥将密文数据还原成明文数据，称为解密。

密钥加密技术分为对称密钥加密和非对称密钥加密两类。对称加密技术是在加密与解密过程中使用相同的密钥加以控制，它的保密度主要取决于对密钥的保密。它的特点是数字运算量小，加密速度快，弱点是密钥管理困难，一旦密钥泄露，将直接影响到信息的安全。非对称密钥加密法是在加密和解密过程中使用不同的密钥加以控制，加密密钥是公开的，解密密钥是保密的。它的保密度依赖于从公开的加密密钥或密文与明文的对照推算解密密钥在计算上的不可能性。算法的核心是运用一种特殊的数学函数——单向陷门函数，即从一个方向求值是容易的，但其逆向计算却很困难，从而在实际上成为不可能。

除了密钥加密技术外，还有数据加密技术。一是链路加密技术。链路加密是对通信线路加密；二是节点加密技术。节点加密是指对存储在节点内的文件和数据库信息进行的加密保护。

3.数字签名技术。数字签名（Digital Signature）技术是将摘要用发送者的私钥加密，与原文一起传送给接收者。接收者只有用发送者的公钥才能解密被加密的摘要。在电子商务安全保密系统中，数字签名技术有着特别重要的地位，在电子商务安全服务中的源鉴别、完整性服务、不可否认服务中都要用到数字签名技术。

在书面文件上签名是确认文件的一种手段，其作用有两点，一是因为自己的签名难以否认，从而确认文件已签署这一事实；二是因为签名不易仿冒，从而确定了文件是真的这一事实。数字签名与书面签名有相同相通之处，也能确认两点，一是信息是由签名者发送的，二是信息自签发后到收到为止未曾做过任何修改。这样，数字签名就可用来防止：电子信息因易于修改而有人作伪；冒用别人名义发送信息；发出（收到）信件后又加以否认。

广泛应用的数字签名方法有RSA签名、DSS签名和 Hash签名三种。RSA的最大方便是没有密钥分配问题。公开密钥加密使用两个不同的密钥，其中一个是公开的，另一个是保密的。公开密钥可以保存在系统目录内、未加密的电子邮件信息中、电话黄页上或公告牌里，网上的任何用户都可获得公开密钥。保密密钥是用户专用的，由用户本身持有，它可以对公开密钥加密的信息解密。DSS数字签名是由美国政府颁布实施的，主要用于跟美国做生意的公司。它只是一个签名系统，而且美国不提倡使用任何削弱政府窃听能力的加密软件。Hash签名是最主要的数字签名方法，跟单独签名的RSA数字签名不同，它是将数字签名和要发送的信息捆在一起，所以更适合电子商务。

4.数字时间戳技术。在电子商务交易的文件中，时间是十分重要的信息，是证明文件有效性的主要内容。在签名时加上一个时间标记，即有数字时间戳（Digita Timestamp）的数字签名方案：验证签名的人或以确认签名是来自该小组，却不知道是小组中的哪一个人签署的。指定批准人签名的真实性，其他任何人除了得到该指定人或签名者本人的帮助，否则不能验证签名

（二）网络信忽安全的目标

1.保密性。保密性是指信息不泄露给非授权人、实休和过程，或供其使用的特性。

2.完整性。完整性是指信息未经授权不能被修改、不被破坏、不被插人、不迟延、不乱序和不丢失的特性。对网络信息安全进行攻击的最终目的就是破坏信息的完整性。

3.可用性。可用性是指合法用户访问并能按要求顺序使用信息的特性，即保证合法用户在需要时可以访问到信息

4.可控性。可控性是指授权机构对信息的内容及传播具有控制的能力的特性，可以控制授权范围内的信息流向以及方式。

5.可审查性。在信息交流过程结束后，通信双方不能抵赖曾经做出的行为，也不能否认曾经接收到对方的信息。

网络信息安全面临的问题

1.网络协议和软件的安全缺陷

因特网的基石是TCP/IP协议簇，该协议簇在实现上力求效率，而没有考虑安全因素，因为那样无疑增大代码量，从而降低了TCP/IP的运行效率，所以说TCP/IP本身在设计上就是不安全的。很容易被窃听和欺骗：大多数因特网上的流量是没有加密的，电子邮件口令、文件传输很容易被监听和劫持。很多基于TCP/IP的应用服务都在不同程度上存在着安全问题，这很容易被一些对TCP/IP十分了解的人所利用，一些新的处于测试阶级的服务有更多的安全缺陷。缺乏安全策略：许多站点在防火墙配置上无意识地扩大了访问权限，忽视了这些权限可能会被内部人员滥用，黑客从一些服务中可以获得有用的信息，而网络维护人员却不知道应该禁止这种服务。配置的复杂性：访问控制的配置一般十分复杂，所以很容易被错误配置，从而给黑客以可乘之机。TCP/IP是被公布于世的，了解它的人越多被人破坏的可能性越大。现在，银行之间在专用网上传输数据所用的协议都是保密的，这样就可以有效地防止入侵。当然，人们不能把TCP/IP和其实现代码保密，这样不利于TCP/IP网络的发展。2.黑客攻击手段多样

进人2024年以来，网络罪犯采用翻新分散式阻断服务(DDOS)攻击的手法，用形同互联网黄页的域名系统服务器来发动攻击，扰乱在线商务。宽带网络条件下，常见的拒绝服务攻击方式主要有两种，一是网络黑客蓄意发动的针对服务和网络设备的DDOS攻击;二是用蠕虫病毒等新的攻击方式，造成网络流量急速提高，导致网络设备崩溃，或者造成网络链路的不堪负重。

调查资料显示，2024年初发现企业的系统承受的攻击规模甚于以往，而且来源不是被绑架的“僵尸”电脑，而是出自于域名系统(DNS)服务器。一旦成为DDOS攻击的目标，目标系统不论是网页服务器、域名服务器，还是电子邮件服务器，都会被网络上四面八方的系统传来的巨量信息给淹没。黑客的用意是借人量垃圾信息妨碍系统正常的信息处理，借以切断攻击目标对外的连线。黑客常用“僵尸”电脑连成网络，把大量的查询要求传至开放的DNS服务器，这些查询信息会假装成被巨量信息攻击的目标所传出的，因此DNS服务器会把回应信息传到那个网址。

美国司法部的一项调查资料显示，1998年3月到2024年2月期间，82%的人侵者掌握授权用户或设备的数据。在传统的用户身份认证环境下，外来攻击者仅凭盗取的相关用户身份凭证就能以任何台设备进人网络，即使最严密的用户认证保护系统也很难保护网络安全。另外，由于企业员工可以通过任何一台未经确认和处理的设备，以有效合法的个人身份凭证进入网络，使间谍软件、广告软件、木马程序及其它恶意程序有机可乘，严重威胁网络系统的安全。

有资料显示，最近拉美国家的网络诈骗活动增多，作案手段先进。犯罪活动已经从“现实生活转入虚拟世界”，网上诈骗活动日益增多。3.计算机病毒

本DOCX文档由 www.zciku.com/中词库网 生成，海量范文文档任你选，，为你的工作锦上添花,祝你一臂之力！