# 计算机犯罪

本词条由[“科普中国”百科科学词条编写与应用工作项目](https://baike.baidu.com/science" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%8A%AF%E7%BD%AA/_blank) 审核 。

公安部计算机管理监察司给出的定义是：所谓计算机犯罪，就是在信息活动领域中，利用[计算机信息系统](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E4%BF%A1%E6%81%AF%E7%B3%BB%E7%BB%9F/6317267" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%8A%AF%E7%BD%AA/_blank)或计算机信息知识作为手段，或者针对计算机信息系统，对国家、团体或个人造成危害，依据法律规定，应当予以刑罚处罚的行为。

**中文名**

[计算机犯罪](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%8A%AF%E7%BD%AA" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%8A%AF%E7%BD%AA/_blank)

**外文名**

Computer　Crime

**开    始**

60年代

**对    象**

计算机

**勘查技术**

现场勘查等

## 目录

1. 1 [定义](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%8A%AF%E7%BD%AA/10329398?fr=aladdin" \l "1)
2. 2 [分类](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%8A%AF%E7%BD%AA/10329398?fr=aladdin" \l "2)
3. 3 [侦破设备](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%8A%AF%E7%BD%AA/10329398?fr=aladdin" \l "3)
4. 4 [侦查重点](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%8A%AF%E7%BD%AA/10329398?fr=aladdin" \l "4)
5. 5 [侦查技术](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%8A%AF%E7%BD%AA/10329398?fr=aladdin" \l "5)

## 定义

[编辑](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%8A%AF%E7%BD%AA/javascript:;)

明确界定规制对象是对其进行法律规制的重要一环，新的法律领域的出现总是不可避免地涉及到对某一类犯罪的正确定义与识别问题。 当学者们首次讨论有关计算机滥用行为的立法时，也很快意识到了这个问题。 统一的计算机犯罪的定义，无论是对执法者来说，还是对一般的工商企业来说，都是大有裨益的。 明确界定规制对象是对其进行法律规制的重要一环，新的法律领域的出现总是不可避免地涉及到对某一类犯罪的正确定义与识别问题。

公安部计算机管理监察司给出的定义是：所谓计算机犯罪，就是在信息活动领域中，利用[计算机信息系统](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E4%BF%A1%E6%81%AF%E7%B3%BB%E7%BB%9F" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%8A%AF%E7%BD%AA/_blank)或计算机信息知识作为手段，或者针对计算机信息系统，对国家、团体或个人造成危害，依据法律规定，应当予以刑罚处罚的行为。

## 分类

[编辑](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%8A%AF%E7%BD%AA/javascript:;)

计算机犯罪分为三大类：

（1）以计算机为犯罪对象的犯罪，如行为人针对个人电脑或网络发动攻击，这些攻击包括“非法访问存储在目标计算机或网络上的信息，或非法破坏这些信息；窃取他人的电子身份等”；

（2）以计算机作为攻击主体的犯罪，如当计算机是犯罪现场、财产损失的源头、原因或特定形式时，常见的有黑客、特洛伊木马、蠕虫、传播病毒和逻辑炸弹等；

（3）以计算机作为犯罪工具的传统犯罪，如使用计算机系统盗窃他人信用卡信息，或者通过连接互联网的计算机存储、传播淫秽物品、传播儿童色情等 [1]  。

## 侦破设备

[编辑](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%8A%AF%E7%BD%AA/javascript:;)

[](https://baike.baidu.com/pic/è®¡ç®æºç¯ç½ª/10329398/0/3853ad1b397194518618bfce?fr=lemma%26ct=single)计算机取证设备Data Compass数据指南针

由于计算机犯罪的特殊性，要侦破计算机犯罪案件，关键就在于提取计算机犯罪分子遗留的[电子证据](https://baike.baidu.com/item/%E7%94%B5%E5%AD%90%E8%AF%81%E6%8D%AE/3448262" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%8A%AF%E7%BD%AA/_blank)。而电子证据具有易删除、易篡改、易丢失等特性，为确保电子证据的原始性、真实性、合法性，在电子证据的收集时应采用专业的数据复制[备份](https://baike.baidu.com/item/%E5%A4%87%E4%BB%BD" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%8A%AF%E7%BD%AA/_blank)设备将电子证据文件复制备份，要求数据复制设备需具备只读设计以及自动校准等功能。

目前国内的[计算机取证设备](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E5%8F%96%E8%AF%81%E8%AE%BE%E5%A4%87" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%8A%AF%E7%BD%AA/_blank)不少，包括Data Copy King多功能复制擦除检测一体机（简称DCK硬盘复制机）、Data Compass[数据指南针](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E6%8C%87%E5%8D%97%E9%92%88/514789" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%8A%AF%E7%BD%AA/_blank)（简称DC）、[网警](https://baike.baidu.com/item/%E7%BD%91%E8%AD%A6/10819437" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%8A%AF%E7%BD%AA/_blank)计算机犯罪取证勘察箱等。其中由[国家高新技术企业](https://baike.baidu.com/item/%E5%9B%BD%E5%AE%B6%E9%AB%98%E6%96%B0%E6%8A%80%E6%9C%AF%E4%BC%81%E4%B8%9A" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%8A%AF%E7%BD%AA/_blank)[效率源](https://baike.baidu.com/item/%E6%95%88%E7%8E%87%E6%BA%90/8820617" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%8A%AF%E7%BD%AA/_blank)历时三年研发的DCK[硬盘复制机](https://baike.baidu.com/item/%E7%A1%AC%E7%9B%98%E5%A4%8D%E5%88%B6%E6%9C%BA/10197282" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%8A%AF%E7%BD%AA/_blank)不仅硬盘复制速度达到创记录的7GB/min，遥遥领先于其他计算机取证设备，同时该硬盘复制机还具备8GB/min的[数据销毁](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E9%94%80%E6%AF%81/3347793" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%8A%AF%E7%BD%AA/_blank)功能，以及硬盘检测、Log日志记录生成、只读口设计等，可自动发现解锁HPA、DCO隐藏数据区，在将嫌疑硬盘中的数据完整复制到目标硬盘的同时，确保取证数据的全面客观。

## 侦查重点

[编辑](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%8A%AF%E7%BD%AA/javascript:;)

针对不同类型的以计算机作为工具实施的犯罪等犯罪，采用的侦查手段也应当分门别类，有序划归。就侦查的步骤不外乎以下几点：现场勘查；证据、材料确定是否立案；分析案情，制定侦查计划；扣押、鉴定证据；缩小侦破案、侦查终结。就目前几类典型计算机犯罪类型的侦查重点和要求而言，有以下几个方面：

**非法侵入计算机信息系统类型案件的侦查重点及要求**

这方面包括日志文件分析、电子文档对比查询、IP 定位、电子证据的提取和保全、日常管理、监督和检查。许多互联网使用单位和个人安全意识淡薄，存在“重应用、轻安全，重实效、轻管理”的情况，如用户密码过于简单、服务器系统没有及时下载升级补丁等，这就要求公安机关充分发挥监督管理的职责，尤其是对重点单位，要加强检查和监督。

**破坏计算机信息系统类型案件的侦查重点及要求**

对破坏信息系统罪的侦查重点一般体现在：一是及时发现犯罪人的作案手段，侦查人员要从技术上突破现有的禁锢；二是设计侦查实验；三是获取间接证据。侦查人员需从环境、技术、动机目的和已获得的人证、物证来综合分析，以作案手段为基础，建立以电子证据为核心的间接证据系统，确定犯罪嫌疑人。

**非法制作、传播计算机病毒类型案件的侦查重点及要求**

对于该类案件的侦查难度也较大，在开展侦查活动中重点应放在破译源代码、获取间接证据方面，同时，由于该类案件的侦查难度较大，在进行常规的侦查措施的同时，必要时还应该聘请专门从事研究计算机病毒方面的专家进行协助调查。我们的侦查人员不仅要掌握先进的科学技术手段，而且还需要熟练应用各种传统的侦查手段。

**以计算机作为工具实施的犯罪的侦查重点及要求**

对盗用网络设备及各种资源的犯罪以计算机作为工具实施的犯罪的侦查重点及要求对盗用网络设备及各种资源的犯罪，应该对案件进行谨慎的排查，仔细的分析可能存在的电子证据和漏洞破绽，必要时也需聘请相关的计算机专业人员协助调查；对侵吞公私财产类型案件的侦查应把重点放在对日志文件、管理记录的分析，可以从管理记录中发现人员的上机、上网等情况；对利用互联网制作、传播淫秽物品类型犯罪行为的侦查应加强对互联网信息的监控，及时、有效地提取证据。

## 侦查技术

[编辑](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%8A%AF%E7%BD%AA/javascript:;)

**现场勘查类技术**

现场勘查类技术分为八类。包括数据的复原技术、数据监控技术、数据加解密技术、数据复制技术、数据欺骗技术、扫描技术、数据截取技术和数据隐藏技术等等。

**证据分析类技术**

证据分析阶段的工作重点是对已收集的证据进行检查和分析，找出与犯罪行为的关联关系，以证明案件事实。证据分析类技术主要包括日志分析技术、对比搜索技术、数据挖掘技术、攻击源追踪技术等，使得入侵追踪系统的分布性取得了实现的基础。

**证据保全类技术**

证据保全工作是指对已获取的证据进行保管，并确保其数据完整性、保密性、抗抵赖性不被破坏。属于证据保存类的技术有数据复制技术、数据加密技术和数字签名技术和数字时间戳技术、数字摘要技术 [2]  。