教育部高等学校信息安全专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

360企业安全集团组织编写

网络空间安全重点规划丛书

顾问委员会主任：沈昌祥 编委会主任：封化民

日志审计与分析

杨东晓 张锋 朱保健 魏昕 编著

Cyberspace Security

根据教育部高等学校信息安全专业教学指导委员会编制的
《高等学校信息安全专业指导性专业规范》组织编写

清华大学出版社

教育部高等学校信息安全专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

网络空间安全重点规划丛书

日志审计与分析

杨东晓 张锋 朱保健 魏昕 编著

清华大学出版社
北京

内 容 简 介

本书共分为7章，分别介绍了日志、日志审计和日志收集与分析系统的相关基础知识，日志收集阶段的对象和方式，日志存储阶段的存储策略和方法，事件过滤和归一化使用的方法及效果，关联分析中的实时关联分析、事件关联分析、告警响应分析和实时统计分析，查询与报表等日志的处理方式，最后结合具体案例对背景需求和解决方案进行了讨论和解读，帮助读者更好地掌握日志审计与分析。

本书每章后均附有思考题总结本章知识点，以便为读者进一步阅读提供思路。

本书由360企业安全集团针对高校网络空间安全专业的教学规划组织编写，既适合作为网络空间安全、信息安全等相关专业的教材，也适合负责网络安全运维的网络管理人员和对网络空间安全感兴趣的读者作为基础读物。

本书封面贴有清华大学出版社防伪标签，无标签者不得销售。
版权所有，侵权必究。侵权举报电话：010-62782989　13701121933

图书在版编目(CIP)数据

日志审计与分析/杨东晓等编著. —北京：清华大学出版社，2019
(网络空间安全重点规划丛书)
ISBN 978-7-302-51744-3

Ⅰ. ①日… Ⅱ. ①杨… Ⅲ. ①计算机网络管理—教材 Ⅳ. ①TP393.07

中国版本图书馆CIP数据核字(2018)第271370号

责任编辑：张　民　常建丽
封面设计：常雪影
责任校对：时翠兰
责任印制：杨　艳

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：8.5　　**字　　数**：189千字
版　　次：2019年2月第1版　　**印　　次**：2019年2月第1次印刷
定　　价：29.00元

产品编号：080633-01

网络空间安全重点规划丛书

编审委员会

顾问委员会主任：沈昌祥（中国工程院院士）

特别顾问：姚期智（美国国家科学院院士、美国人文及科学院院士、中国科学院院士、“图灵奖”获得者）

何德全（中国工程院院士）　蔡吉人（中国工程院院士）

方滨兴（中国工程院院士）　吴建平（中国工程院院士）

王小云（中国科学院院士）

主　　任：封化民

副 主 任：韩　臻　李建华　张焕国　冯登国

委　　员：（按姓氏拼音为序）

蔡晶晶　曹珍富　陈克非　陈兴蜀　杜瑞颖　杜跃进

段海新　范　红　高　岭　宫　力　谷大武　何大可

侯整风　胡爱群　胡道元　黄继武　黄刘生　荆继武

寇卫东　来学嘉　李　晖　刘建伟　刘建亚　马建峰

毛文波　潘柱廷　裴定一　钱德沛　秦玉海　秦志光

卿斯汉　仇保利　任　奎　石文昌　汪烈军　王怀民

王劲松　王　军　王丽娜　王美琴　王清贤　王新梅

王育民　吴晓平　吴云坤　徐　明　许　进　徐文渊

严　明　杨　波　杨　庚　杨义先　俞能海　张功萱

张红旗　张宏莉　张敏情　张玉清　郑　东　周福才

左英男

丛书策划：张　民

出版说明

21世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它会直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，全球对信息安全人才的需求量不断增加，但我国目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会对信息安全人才的需求。为此，教育部继2001年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信、物理、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家肖国镇教授担任编委会主任，指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。系列教材的作者都是既在本专业领域有深厚的学术造诣、又在教学第一线有丰富的教学经验的学者、专家。

该系列教材是我国第一套专门针对信息安全专业的教材，其特点是：

① 体系完整、结构合理、内容先进。

② 适应面广：能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套：除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时，紧跟科学技术的新发展。

在全力做好本版教材，满足学生用书的基础上，还经由专家的推荐和审定，遴选了一批国外信息安全领域优秀的教材加入到系列教材中，以进一步满足大家对外版书的需求。“高等院校信息安全专业系列教材”已于2006年年初正式列入普通高等教育“十一五”国家级教材规划。

此为试读，需要完整PDF请访问：www.ertongbook.com

2007 年 6 月，教育部高等学校信息安全类专业教学指导委员会成立大会暨第一次会议在北京胜利召开。本次会议由教育部高等学校信息安全类专业教学指导委员会主任单位北京工业大学和北京电子科技学院主办，清华大学出版社协办。教育部高等学校信息安全类专业教学指导委员会的成立对我国信息安全专业的发展起到重要的指导和推动作用。2006 年教育部给武汉大学下达了“信息安全专业指导性专业规范研制”的教学科研项目。2007 年起该项目由教育部高等学校信息安全类专业教学指导委员会组织实施。在高教司和教指委的指导下，项目组团结一致，努力工作，克服困难，历时 5 年，制定出我国第一个信息安全专业指导性专业规范，于 2012 年年底通过经教育部高等教育司理工科教育处授权组织的专家组评审，并且已经得到武汉大学等许多高校的实际使用。2013 年，新一届“教育部高等学校信息安全专业教学指导委员会”成立。经组织审查和研究决定，2014 年以“教育部高等学校信息安全专业教学指导委员会”的名义正式发布《高等学校信息安全专业指导性专业规范》(由清华大学出版社正式出版)。

2015 年 6 月，国务院学位委员会、教育部出台增设“网络空间安全”为一级学科的决定，将高校培养网络空间安全人才提到新的高度。2016 年 6 月，中央网络安全和信息化领导小组办公室(下文简称中央网信办)、国家发展和改革委员会、教育部、科学技术部、工业和信息化部及人力资源和社会保障部六大部门联合发布《关于加强网络安全学科建设和人才培养的意见》(中网办发文[2016]4 号)。为贯彻落实《关于加强网络安全学科建设和人才培养的意见》，进一步深化高等教育教学改革，促进网络安全学科专业建设和人才培养，促进网络空间安全相关核心课程和教材建设，在教育部高等学校信息安全专业教学指导委员会和中央网信办资助的网络空间安全教材建设课题组的指导下，启动了“网络空间安全重点规划丛书”的工作，由教育部高等学校信息安全专业教学指导委员会秘书长封化民校长担任编委会主任。本规划丛书基于“高等院校信息安全专业系列教材”坚实的工作基础和成果、阵容强大的编审委员会和优秀的作者队伍，目前已经有多本图书获得教育部和中央网信办等机构评选的“普通高等教育本科国家级规划教材”“普通高等教育精品教材”“中国大学出版社图书奖”和“国家网络安全优秀教材奖”等多个奖项。

“网络空间安全重点规划丛书”将根据《高等学校信息安全专业指导性专业规范》(及后续版本)和相关教材建设课题组的研究成果不断更新和扩展，进一步体现科学性、系统性和新颖性，及时反映教学改革和课程建设的新成果，并随着我国网络空间安全学科的发展不断完善，力争为我国网络空间安全相关学科专业的本科和研究生教材建设、学术出版与人才培养做出更大的贡献。

我们的 E-mail 地址是：zhangm@tup.tsinghua.edu.cn，联系人：张民。

“网络空间安全重点规划丛书”编审委员会

前言

没有网络安全，就没有国家安全；没有网络安全人才，就没有网络安全。

从更多、更快、更好地培养网络安全人才出发，如今，许多学校都在下大工夫、花大本钱，聘请优秀老师，招收优秀学生，着力培养一流的网络安全人才。

网络空间安全专业建设需要体系化的培养方案、系统化的专业教材和专业化的师资队伍。优秀教材是网络空间安全专业人才的关键。但是，这是一项十分艰巨的任务。原因有二：其一，网络空间安全的涉及面非常广，至少包括密码学、数学、计算机、操作系统、通信工程、信息工程、数据库、硬件等多门学科。因此，其知识体系庞杂、难以梳理；其二，网络空间安全的实践性很强，技术发展更新非常快，对环境和师资要求也很高。

“日志审计与分析”是网络空间安全和信息安全专业的基础课程，通过日志各知识点的介绍掌握日志审计与分析。本书涉及的知识面宽，共分为7章。

第1章介绍日志基本知识，第2章介绍日志收集，第3章介绍事件归一化，第4章介绍日志存储，第5章介绍关联分析，第6章介绍查询与报表，第7章介绍典型案例。

本书既可作为网络空间安全、信息安全等相关专业的教材和参考资料，也可作为网络安全研究人员的入门基础读物。随着新技术的不断发展，今后将不断更新本书中的内容。

在本书的编写过程中，得到了360企业安全集团的裴智勇、翟胜军、杨进国，北京邮电大学雷敏等专家、学者的鼎力支持，在此对他们的工作表示衷心感谢！

由于作者水平有限，书中难免存在疏漏和不妥之处，欢迎读者批评指正。

作　者

2018年12月

目录

此为试读，需要完整PDF请访问：www.ertongbook.com

第1章 日志基本知识

日志(log)是由各种不同的实体产生的“事件记录”的集合。日志记录是将事件记录收集到日志中的行为,主要分为安全日志记录、运营日志记录、依从性日志记录和应用程序调试日志记录4种基本类型。日志详细记录了谁在什么时间对某个对象进行了何种操作所产生的变化。

日志可以帮助系统进行排错和优化。在安全领域,日志可以用于故障检测和入侵检测,反映安全攻击行为,如登录错误、异常访问等。日志不仅是在事故发生后查明“发生了什么”的一个很好的“取证”信息来源,还可以为审计进行跟踪。此外,安全管理人员可以根据网络安全日志进行安全追踪和溯源,并进行调查取证,从而实现设备的安全运营。其主要作用有以下3个。

(1) 根据网络安全日志可以安全追踪和溯源。

(2) 根据日志原始记录信息进行调查取证。

(3) 根据运维日志实现设备安全运维。

本章主要介绍日志的基础知识。通过本章的学习,理解日志设备产生的原因、日志管理设备的定义、日志审计的基本概念和相关的法律法规、日志收集与分析系统的基本概念以及日志全生命周期的管理。

1.1 日志概述

1.1.1 日志设备产生的原因

随着网络规模的不断扩大,网络中的设备数量和服务类型越来越多,这给系统的安全性和稳定性带来了各种挑战。因此,急需对系统中硬件、软件、系统数据的增、删、改、查以及对系统问题进行记录,从而可以有效地掌握系统安全状况和运行情况,及时发现系统异常并快速定位、解决问题、补救损失。与此同时,长期以来,各种安全事件呈几何级增长,来自外部的攻击入侵事件频发,而且这些安全事件呈现出“组织性”“针对性”和“目的性”等特点,给公民的财产造成巨大损失,给人们的日常工作和生活带来极大威胁。因此,要及时发现这些异常并进行防范或者在发生网络入侵之后使损失最小化,就需要对网络中的各种事件信息进行记录和分析。

日志通常是计算机系统、设备、软件等在某种情况下记录的信息,它可以记录系统产

生的所有行为并按照某种规范将这些行为表达出来。这些信息可以帮助系统排错、优化系统的性能，管理者还可以根据这些信息调整系统的行为。在安全领域，日志主要用于描述网络中所发生事件的信息，包括性能信息、故障检测和入侵检测，这些信息可以反映出很多安全攻击行为，如登录错误、异常访问等。日志是在事故发生后查明“发生了什么”的一个很好的“取证”信息来源。

日志在维护系统稳定性和安全防护方面都起到了非常重要的作用，由此，对日志进行专门记录和管理的设备应运而生，各种不同的网络设备、复杂的应用系统以及数据库等每天都会以各自的标准记录大量相关的日志。这些日志可以通过专门的管理设备进行管理，这些设备称为日志管理设备。

1.1.2 日志管理设备的定义

日志设备是指产生“事件记录”的各种设备，包括网络设备、计算机系统、数据库或者应用程序等。企业信息系统中会包含多种日志设备，如路由器、防火墙、入侵检测系统/入侵防御系统（Intrusion Detection System/Intrusion Protection System，IDS/IPS）、交换机、服务器和数据库等。以下对常见的日志设备进行简要介绍，详细内容将在第 2 章展开介绍。

网络设备及部件是连接到网络中的物理实体。网络设备的种类繁多，且与日俱增。基本的网络设备有：计算机（无论其为个人计算机或服务器）、集线器、交换机、网桥、路由器、网关、网络接口卡（Network Interface Card，NIC）、无线接入点（Wireless Access Point，WAP）、打印机和调制解调器、光纤收发器、光缆等。

计算机系统由计算机硬件和软件两部分组成。硬件包括中央处理器、存储器和外部设备等；软件是计算机的运行程序和相应的文档。计算机系统具有接收和存储信息、按程序快速计算和判断并输出处理结果等功能。常见的系统有 Windows、Linux 等。

数据库（database）是建立在计算机存储设备上的按照数据结构组织、存储和管理数据的仓库，用户可以对文件中的数据进行新增、截取、更新、删除等操作。

应用程序指为完成某项或多项特定工作的计算机程序。

由于日志的种类很多，生成日志的设备多种多样，所以很难定义单一的标准用于日志记录。通常，日志设备记录的日志应该包含如下基本信息。

- 对事件内容辅以适当的细节。
- 事件发生的开始时间和结束时间。
- 事件发生的位置（哪个主机、什么文件系统、哪个网络接口等）。
- 参与者。
- 参与者来源。

日志设备还可以记录其他更多与事件相关的详细信息。

传统的日志能够反映出系统运行的状态变化，同时能够对端口扫描、口令破解等安全事件进行记录。现有的部分安全产品能够将多条日志进行关联分析，从而得到安全事件。由于日志能够对系统运行中的特定活动进行记录，系统管理人员和安全分析者从日志分

析和系统安全的角度出发，可归纳出日志具有以下特点。

(1) 日志格式具有多样性。

目前国际上尚未制定出统一的日志格式标准，不同厂商根据自身需求制定相应的日志格式，故市场上出现了多种类型的日志。

(2) 日志数据量很大。

由于日志对每一个事件均进行记录，因此，无论是操作系统，还是网络设备都会产生大量的日志记录，大型企业的防火墙、IDS 等设备每天可产生多达数十 G 的日志文件。

(3) 网络设备日志具有时空关联性。

针对某个特定的网络攻击事件，不同的安全设备通常都会进行记录。例如，一个分布式拒绝服务(Distributed Denial of Service，DDoS)攻击会同时在防火墙和 IDS 日志中留下痕迹。因此，结合多个设备日志，采用数据挖掘算法找出日志之间的时空关联性，有助于提取出网络安全事件。

(4) 日志信息容易被篡改。

计算机系统和相关设备的日志是以文本的形式存储的，并且没有对日志进行有效的保护，网络入侵者可能对日志信息进行篡改或直接删除，因此存在较大的安全隐患。

(5) 分析和获取日志数据困难。

不同设备的日志格式差异很大，部分设备日志信息需要专用的工具才能查看，给日志的分析带来了很大困难。

基于上述日志的特点，需要通过专门的管理设备对日志进行管理，从而实现对日志信息的实时监控和审计整个系统的运行状况，这些设备称为日志管理设备。日志管理设备是对全网范围内的主机、服务器、网络设备、数据库以及各种应用服务系统等产生的日志进行全面收集、实现日志的集中管理和存储并进行细致分析的设备，支持解析任意格式、任意来源的日志。

1.1.3　日志的作用

1. 安全日志审计：网络追踪溯源

网络追踪溯源是指确定网络攻击者身份或位置及其中间介质的过程。身份指攻击者名字、账号或与之有关系的类似信息；位置包括其地理位置或虚拟地址，如 IP 地址、MAC 地址等。追踪溯源过程还能够提供其他辅助信息，如攻击路径和攻击时序等。网络管理者可使用追踪溯源技术定位真正的攻击源，以采取多种安全策略和手段，从源头抑制，防止网络攻击带来更大的破坏，并记录攻击过程，为司法取证提供必要的信息支撑。在网络中应用追踪溯源可以：

- 确定攻击源，制定实施针对性的防御策略。
- 确定攻击源，采取拦截、隔离等手段，减轻损害，保证网络平稳健康地运行。
- 确定攻击源，记录攻击过程，为司法取证提供有力证据。

网络管理人员采用网络追踪溯源技术，调取并分析事件发生前后一段时间的日志，可以发现攻击者的一系列行为及其攻击手段。调取的日志内容包含所发生问题的认证日

志、服务器操作日志、攻击事件日志等与安全相关的日志。

2. 运维日志：安全运维

运维日志分析是企业网络运维管理的核心部分。通过运维通道集中、网络运维日志详细记录，可合理安排网络运维工作，实现运维人员工作的量化管理，提高运维管理要求落地的自动化水平和强制化能力。

(1) 运维故障回溯。日志集中管理系统及审计系统详细记录了运维人员的日常运维操作，可通过操作命令回放方式实现日常运维操作重现。对于人为操作故障，通过日志回放分析，可进行操作追溯，定位故障原因。

(2) 运维经验固化。通过日志集中管理及审计系统记录的运维操作指令流，可完整模拟日常运维操作。对于典型维护操作场景，可将回放作为某类设备配置参考，将优秀运维人员的维护经验固化，全网推广。对于例行维护操作，可通过日志分析“提取→固定→自动化”进一步提高效率。还可将固化的典型维护操作作为新员工培训教材，实现运维知识的有效传递。

(3) 运维工作量化。对于指令标准化程度高的网元，通过对日志以时间、网元、账号等维度的分析，可有效衡量运维人员的日常工作量，解决运维工作难以量化的问题。

(4) 运维要求核查。网络运维中很重要的一项工作是操作维护作业计划。但在实际管理中，虽然可查看操作维护记录，但对操作人员是否执行相关维护作业计划、执行结果如何，却缺乏有效的核查手段。通过日志集中管理及审计系统记录的操作记录，可对维护作业计划的执行时间、频次、结果进行有效的核查。

(5) 合理安排运维工作。根据日志系统统计的运维人员工作量，合理安排维护人员维护网元数量。

3. 合规类日志：调查取证

取证是在事件发生后重建“发生了什么”情景的过程。这种描述往往基于不完整的信息，而信息可信度是至关重要的。日志是取证过程中不可或缺的组成部分。

日志一经记录，就不会因为系统的正常使用而被修改，这意味着这是一种“永久性”的记录。因此，日志可以为系统中其他可能更容易被更改或破坏的数据提供准确的补充。

每条日志中通常都有时间戳，提供每个事件的时间顺序。而且，日志通常会被及时发送到另一台主机(通常是一个集中日志收集器)，这也提供了独立于原始来源的一个证据来源。如果原始来源上信息的准确性遭到质疑(例如，入侵者篡改或者删除了日志)，独立的信息源可能被认为是更可靠的附加来源。同样，不同来源甚至不同站点的日志可以佐证其他证据，提高每个源的准确性。

日志有助于加强收集到的其他证据。重现事件往往不是基于一部分信息或者单个信息源，而是基于来自各种来源的数据，包括文件和各子系统上的时间戳、用户的命令历史记录、网络数据和日志。

通过日志审计，协助系统管理员在受到攻击，或者发生重大安全事件后查看网络日

志，从而评估网络配置的合理性、安全策略的有效性，追溯分析安全攻击轨迹，并能为实时防御提供手段。通过对人员的网络行为审计，确认其行为的合规性，确保上网行为管理的安全。

1.2 日志审计

1.2.1 信息系统审计概念

信息系统审计的发展是随着审计理论和计算机理论的不断完善而发展起来的，其发展过程大致可分为起步阶段、快速发展阶段、成熟阶段和普及阶段。

1. 1960—1970 年：信息系统审计的起步阶段

这一时期，随着计算机在各个行业的广泛运用，会计操作也从纸质凭证向电子化发展，审计人员开始意识到计算机环境下开展审计业务的优势，逐渐形成了信息系统审计。但总的来说，这一时期信息系统审计还仅处于新生阶段，专业人员对信息系统审计的认识比较匮乏。

2. 1970—1980 年：信息系统审计的快速发展阶段

这一时期，计算机技术和审计理论进一步发展，计算机在各个行业、各种业务中得到更广泛的运用，计算机数据处理方法和管理信息系统也被越来越多的人认可，信息系统理论和实务方面都得到了很大的进步。在实践中，计算机辅助审计的作用也日益突出，信息系统审计进入发展阶段。

3. 1980—1990 年：信息系统审计的成熟阶段

随着计算机技术的日益完善，在审计过程中大规模地运用计算机技术也不再罕见，然而，计算机技术在带给审计人员便利的同时，也带来很多计算机犯罪案件。这使得审计部门意识到信息系统防范体系还不够成熟，人们逐渐意识到信息系统审计的重要性。1981 年，美国电子数据处理协会开始组织注册信息系统审计师执业考试，这一考试的出现标志着信息系统审计步入成熟阶段。同一时期，日本先后派遣学者前往美国学习信息系统审计理论和实务，于 1985 年也出台了《系统审计标准》，并开展“系统审计师”考试，这标志亚洲信息系统审计也步入了成熟阶段。

4. 1990 年以后：信息系统审计的普及阶段

这一时期，信息技术进入大爆炸时期，信息系统的发展呈现出其特有的复杂化和网络化的特征。信息系统审计在很多发达国家已经进入普及阶段。1994 年，电子数据处理审计师协会顺应时代发展的脚步，更名为信息系统审计与控制协会，从此，该协会也成为审计工作者从事信息系统审计的唯一国际组织。尽管信息系统审计已经进入普及期，但是我们也不难看出信息系统审计还存在很多不足，特别是在外界环境不断变化的大数据时

代，需要更多专业的审计人员为信息系统审计而努力，让信息系统审计不断优化。

信息系统审计逐渐得到越来越多的国家和部门的重视，是因为有其存在的必要性。具体来说：首先，信息系统审计是公司治理的重要举措。在计算机技术发展刚刚开始的阶段，信息系统只是作为一种后台支撑的技术手段而存在。但是，随着计算机水平的不断提高，信息系统已经逐渐转变其功能，成为各个企业之间竞争的重要筹码。因此，信息系统审计就显得格外重要，对信息系统进行审计可以确保被审计单位信息系统得到高效运转，并根据审计结果为管理层提出相应的改进措施，促进企业不断提高其竞争力，实现利润最大化。其次，信息系统审计是保证企业信息化发展的必然选择。随着计算机运用范围的不断扩大，计算机水平的提高，会计做账方式也从手工做账发展到通过计算机软件进行账务处理，这就促使了计算机审计的产生。计算机审计使得审计方法从手工人工的实际操作发展到计算机水平。但是，随着计算机水平的不断进步，信息系统涵盖的内容越来越多，从最基本的信息存储到数据分析都可以在信息系统中完成，这就使得计算机审计已经不能满足审计目标的完成。因此，信息系统审计应运而生。信息系统审计能够对信息系统从开发使用到最后的维护等整个生命周期都进行审核，提高了审计的范围，增强了审计的安全性和可靠性。

信息系统审计是一个通过收集和评价审计证据，对信息系统是否能够保护资产的安全、维护数据的完整、有效实现被审计单位的目标、使组织的资源得到高效使用等方面做出判断的过程。国际通用的 CC 准则（即 ISO/IEC 15408-2：1999《信息技术安全性评估准则》）中给出了信息系统安全审计（Information System Security Audit，ISSA）的明确定义：信息系统安全审计主要是指对与安全有关活动的相关信息进行识别、记录、存储和分析；审计记录的结果用于检查网络上发生了哪些与安全有关的活动以及这些活动的负责主体是什么。审计的主要功能包括：安全审计自动响应、安全审计数据生成、安全审计分析、安全审计浏览、安全审计事件选择、安全审计事件存储等。

通俗地说，信息安全审计就是信息网络中的“监控摄像头”，通过运用各种技术手段监控网络信息系统中的各种活动，记录分析网络中的各种可疑行为、违规操作、敏感信息，帮助定位安全事件源头和追查取证，防范和发现计算机网络犯罪活动，为信息系统安全策略制定、风险内控提供有力的数据支撑。

信息系统审计过程与一般审计过程一样，分为准备阶段、实施阶段和报告阶段。其中，准备阶段和报告阶段涉及的技术方法与财务审计运用的技术方法区别不大，而实施阶段涉及的技术方法则具有信息技术的特色。在实施阶段，针对被审计的信息系统，审计人员开展的工作可以分为 3 个层次：了解、描述和测试。

计算机信息系统环境下审计技术方法与手工环境下传统的审计技术方法相比，增加了计算机技术的内容。信息系统审计方法既包括一般方法（即手工方法），也包括应用计算机审计的方法。信息系统审计的一般方法主要用于对信息系统的了解和描述，包括面谈法、系统文档审阅法、观察法、计算机系统文字描述法、表格描述法、图形描述法等。应

此为试读，需要完整PDF请访问：www.ertongbook.com