XINXIXITON

GJIANCHAJ

JISHUZHINAN

XINXIXITONGJIAN

CHAJISHU

ZHINAN

XINXIXITONGJIAN

CHAJISHUZHINAN

XINXIXITONGJIANCHAJISHU

信息系统监查技术指南

胡克瑾　编著

同济大学出版社

内 容 提 要

实施信息系统监查，确保信息系统的安全、可靠和有效是信息化的基础，是健全地进入信息化社会的不可缺少的重要环节。本书作者通过对国外先进的系统监查标准与方法的研究分析，从系统监查的基本概念开始，较全面、系统地论述了信息系统监查的一般标准、信息系统计划、开发、运行各阶段的监查实施标准和监查报告标准，最后还介绍了几种系统监查的技术与方法。书末附有与系统监查相关的法规和计算机系统安全对策标准。

本书可作为管理科学与工程专业的本科生或研究生的教材或教学参考书，也可供信息系统的管理人员和从事系统监查的人员参考。

责任编辑 吴味隆

封面设计 李志云

信息系统监查技术指南

胡克瑾 编著

同济大学出版社出版

（上海四平路 1239 号 邮编 200092）

新华书店上海发行所发行

同济大学印刷厂印刷

开本：850 × 1168 1/32 印张：5.75 字数：160 千字

1997 年 12 月第 1 版 1997 年 12 月第 1 次印刷

印数：1—3000 定价：10.00 元

ISBN7-5608-1883-8/TP·198

序

当今世界，正向着信息化时代迈进，大力发展信息产业，广泛推广信息技术的应用，推进信息化进程，这是时代赋于我们的重任。纵观国际经济形势，信息化已成为当今世界的潮流，经济发达国家都将信息产业作为整个社会经济发展的基础，以计算机为中心的信息系统逐渐渗透到社会活动、经济活动和人民生活等各个方面。计算机、通信、网络的互相结合，使大量的信息系统发展成相互沟通的大系统、大网络、大体系，这将使应用更为方便，但同时也使系统变得更为庞大、更为复杂，并也导致了社会、企业等对信息系统的极大的依附性。也就是说，当信息系统发生故障、停止运行或系统发生错误而丧失其有效功能时，该领域的各种活动就失去了支撑和保障，甚至还要影响到社会、生活等许多方面。因此，实施信息系统监查，确保信息系统的可靠、安全及有效是信息化的基础，已成为健全地进入信息化社会必不可少的重要环节，并在推进信息化进程中越来越受到国际、国内有关人士的关注。

美国是在计算机进入实用阶段时开始提出系统监查(System Audit)的，其成立的全美系统监查人协会(EDPAA)从事系统监查活动已有 25 ~ 30 年的历史。日本的系统监查从 80 年代初开始，1985 年通产省公开发表“系统监查标准”，并着手培养从事系统监查的骨干队伍，并出版《系统监查指南》、《系统监查技术》等书籍。近几年，东南亚各国，包括泰国等国也制定了有关法规，成立专门机构，作为开展系统监查业务的中心。

在我国向信息化社会迈进的今天，计算机应用越来越普及，大量信息系统不断推出，企业的管理信息系统从点到面，由单机到系统，由单机到联网迅速发展，效益十分明显。我国要保证在经济、社会和科技方面的稳步发展，计算机的应用必不可少，从而系统监查这项工作势在必行，必须纳入实施我国信息化发展的规划和计划之中。

本书通过对国外先进的系统监查标准与方法的研究与分析，并就监查指南、监查标准、一般标准、实施标准、报告标准、监查实施技术方法等方面提出了观点和看法，供有关部门在开展系统监查工作中参考，以促使信息系统能更安全、更可靠、更有效地运行，从而能为使我国健全地进入信息化社会起到促进和推动作用。

高毓乾

1996.12

前　言

接触“Audit”这个词已有很久历史，最早是从会计审计、帐目稽核和查帐开始的。System Audit 在什么时候、在什么地方开始被用于以计算机为核心的信息系统是不明确的，但从 System Audit 的文献看，系统监查（System Audit）、电子数据处理监查（EDP Audit）和计算机监查（Computer Audit）都是在计算机大量进入实用阶段时开始的。

美国最早在 1954 年从计算机应用于事务处理时开始系统监查。由于计算机的利用，促使业务处理过程的变化，导致内部规则、手续等的改变，原有的内部规则及监查方法产生了问题，不得不开始研究新的监查方法。但是从当时硬件的功能及适应范围看，当时的系统监查只不过是特定的组织，在限定的范围内实施。

60 年代开始，由于计算机的迅速发展，数据处理等的业务范围逐渐扩大，计算机的利用给企业的业务处理带来了极大的影响，产生了一场革命。这不仅是业务处理过程，还包括经营过程及意识方法等的变化。当时是由会计事务所出面对金融机关等进行监查，但还没有作为制度进行实施。IBM 公司出版了《Audit Encounters Electronic Data Processing》、《In-line Elecronic Processing and Audit Trail》等文献，给出了在新的 EDP 环境下的内部监查规则、组织方法，还介绍了许多新的概念、术语及监查技术等，这些文献是该领域中的原典。接着在 1968 年由美国注册会计师协会出版了《会计监查与计算机》一书。60 年代可以说是系统监查的萌芽期，发表

了若干引人注目的研究成果，系统监查是由国际会计事务所进行，实施内外监查。金融机关设立了 EDP 监查人及安全办公室。美国国防部陆海军监查局引入了通用监查软件包。但社会上对系统监查的认识是不够的，系统监查远未普及。

70 年代是系统监查的发展期，由于计算机的应用和电子数据处理的普及，利用计算机犯罪案例的出现，在社会上引起强烈反响，使人们认识到 EDP 监查的必要性。美国注册会计师协会在事件发生的第二年即 1974 年发表了《内部规则的调查与评价对 EDP 的影响》作为对 EDP 实施监查的标准。这是由会计师执行会计监查，把内部监查作为会计师的义务。

1975 年日本信息处理开发协会设立了系统监查委员会，开始了系统监查的研究。通过组织几批访美考察团，了解了美国实施系统监查的情况，并发表了研究报告。

日本注册会计师协会在 1976 年发表了《使用电子计算机的会计组织的内部规则质问书（修订案）》、《EDP 系统的监查标准及监查过程试案》和《EDP 监查方法》等，并明确指出这些不是参考资料，而是监查人必须要执行的标准。

1977 年由美国内部监查人协会发表了有名的《系统可监查性及规则的研究》，通称 SAC 报告，该报告得到 IBM 公司的经济援助，由斯坦福研究院实施调查，在对美国、欧洲、加拿大、日本等地的企业进行调查的基础上进行总结，并对监查方法与监查工具进行了详细的研究。

80 年代是系统监查的成熟期。由于社会的信息化，先进国家大力发展信息产业，加上计算机与通信的结合和计算机网络的普及，使信息系统发展成为相互能沟通的大网络、大系统。这使得计算机的应用更方便、更普及，同时也导致了利用计算机犯罪率的升高。据 1983 年日本的“警察白书”，1971 年至 1982 年日本确认的计算机犯罪案件为 30 件，而全日本利用磁卡欺诈犯罪案件仅 1982 年就上升为 321 件。犯罪率的急剧上升说明信息系统发展了，防

范体制仍很不充分，这就引起了日本政府的极大重视。如何尽早地研究防范体制，制定综合的防范标准，并使之法律化都是急待解决的问题。日本通产省 1982 年在机械信息产业局中设立了“计算机安全研究会”，研究信息化健全发展的必要法制。另外，通产省主管的产业结构审议会情报产业部会，在 1983 年 12 月发表了《有关计算机安全对策》。这是在当年 1 月通产大臣咨询的中间答辩时选定的重要紧急课题“计算机安全的研究”通过近一年的研究后得到的成果。

1984 年，日本政府委托情报化对策委员会系统监查部会对美国的系统监查标准进行研究。翌年，通产省公开发表了《系统监查标准》，提出了“随着信息系统的网络化进展，仅仅是系统内部的监查是不充分的，有必要尽早地引入由具有专门知识与技术的、与系统没有直接关系的第三者（系统监查人）对信息系统的安全全面进行检查……”等的观点，并在全日本的软件水平考试中增添“系统监查人”一级的考试（最高一级，在系统分析员之上），着手培养从事系统监查的骨干队伍。

由于系统监查标准的制定与推广，对信息系统的发展带来明显的效果。据日本 1986 年的调查报告，信息系统的平均无故障时间（MTBF）增加 19%，而平均故障修复时间（MTTR）压缩了 30%。由此可见，系统监查带来的效果是十分明显的。

本书主要参考了《信息化时代的系统监查方法》（青山监查法人编）、《系统监查手册——管理目标与监查实施》（EDP 监查人协会）、《系统监查标准解说》（日本情报处理开发协会）等书籍，引进了日本实施系统监查的模式，详细介绍了日本推行的系统监查标准。

本书从系统监查的基本概念开始，贯穿信息系统各阶段的主线，叙述了一般标准、系统计划开发、运行、维护全过程的监查实施标准和监查报告标准。最后还介绍了几种系统监查的技术与方法。

希望本书的出版对在我国推进信息系统监查略尽绵力，对促使信息系统更有效、更安全、更可靠能够有所帮助，起到实用指南的作用。

不当之处，恳请读者提出宝贵意见。

编　者

1997 年 1 月 26 日

目　录

第一章

系统监查标准

一、标准的提出

1. 目的

随着信息事业的发展，在经济、社会等很多领域出现了与计算机系统紧密依存的局面。另外，由于信息处理技术与通信技术的发展以及相互结合促进了网络技术的发展，将使信息化更广泛更深入地渗透到各个领域。其结果导致了当计算机系统停止运行或错误使用而丧失其有效功能时，该领域从事的经营活动就失去了支撑和保障，甚至还要影响到社会、生活等许多方面。因此，确保计算机系统的可靠性、安全性以及有效性是信息化的基础，是今后能健全地进入信息化社会的不可缺少的课题。

系统监查是指由独立于监查对象的系统监查人员对信息系统进行综合的检查与评价，对有关人员进行参谋和劝告。这是确保安全对策的实施以及促进系统使用的极为有效的方法。

制定本系统监查的标准将促进系统监查的普及。

2. 基本事项

(1) 本标准是对以电子计算机为核心的信息系统进行监查的指南，它列出了监查时的必要事项。

(2) 本标准由一般标准、实施标准以及报告标准三部分组成。

1) 一般标准　表示系统监查的综合事项。决定系统监查的基本目的、对象、系统监查人员、监查时期、监查计划、监查顺序。

2) 实施标准　表示系统监查具体的实施内容。决定系统监查人员从计划业务、开发业务到运行业务各阶段进行监查的方针

与内容。

3) 报告标准　表示系统监查结果的归纳事项。决定监查结果的收集整理及根据监查结果应采取的措施。

(3) 组织体制要配备能够切实实施系统监查的体制。

(4) 系统监查人员要备有系统监查指南等,以便切实运用与业务相应的实施标准。

3. 注意事项

(1) 实施标准要按业务的实际情况进行。

(2) 实施系统监查时要充分利用电子计算机系统安全对策标准。

二、一般标准

项　目	内　容	说明页次
1. 目的	系统监查以提高系统的可靠性、安全性、有效性,健全地进入信息化社会为目的	32
2. 对象	(1) 系统监查的对象是指以电子计算机为核心的信息系统	32
	(2) 系统监查的对象包括与系统计划、开发及运行有关的全部业务	33
3. 系统监查人	(1) 系统监查由系统监查人员实施	34
	(2) 系统监查人员必须独立于被监查的组织与部门	34
	(3) 系统监查人员必须具备下列能力与知识: 1) 有关系统计划与开发的知识 2) 有关系统运行的知识 3) 监查能力 4) 有关实施系统监查的知识	35

续表

项　目	内　容	说明页次
4. 监查时期	(1) 系统计划与开发业务的监查在各业务实施时进行	37
	(2) 运行业务的监查，每隔一定时间实施	37
	(3) 当系统大幅度变更时，实施与开发业务相同的监查	38
5. 监查计划	(1) 制定监查的基本计划与个别计划	39
	(2) 基本计划包括以下各项目：	39
	1) 本年度的监查对象	
	2) 重点监查的课题	
	3) 实施体制	
	4) 年内进度表	
	(3) 个别计划包括以下各项目：	40
	1) 对象	
	2) 目的	
	3) 范围与手续	
	4) 时期与日程	
	5) 负责人与业务分配	
	6) 报告时期	
6. 监查顺序	系统监查根据个别计划按如下顺序进行：	42
	(1) 预备调查	
	(2) 实施调查	
	(3) 评价和结论	

三、实施标准

1. 计划业务

项　　目	内　　容	说明页次
(1) 计划	1) 是否制定系统开发的长期与短期计划，是否定期并且在情况变化时对计划进行相应的调整	44
	2) 是否建立对计划规模和重要性等进行确认的规则；此外这些规则是否得到负责人的认可	44
	3) 计划书中是否包含目的、手段、资金、时期、人员、设备等条文	45
	4) 计划书中是否写明与其他业务配合的系统开发的优先级	46
	5) 计划书中是否记述对系统开发中产生的组织体制变更、业务改变与废除等的对策	46
	6) 计划书中是否记述相应的安全对策	47
(2) 调查、分析	1) 对用户需求的调查，是否确定调查的对象、范围与方法	47
	2) 现状分析是否由用户参加；基础资料的收集以及分析结果的评价是否合适；	48
	3) 技术调查是否包括软硬件、各种内部及外部的技术预测	49
	4) 对电子计算机系统的停止、错误动作是否从发生频率、影响程度、损害额等观点进行分析	49
	5) 是否对系统运行中产生的差错、数据泄漏、破坏和改变、不正当的使用、私有权的侵害等从发生的频率、影响程度、损害金额等观点进行分析	49
	6) 对系统运行有关法律、制度等是否进行全面的调查	50
	7) 对系统运行而受影响的业务、管理体制、各种规定等，包括修正在内是否进行调查研究	50
	8) 在设定系统生存期时作为前提的各种条件是否合适	51

续表

项　目	内　容	说明页次
(3) 开发探讨	1) 实施开发计划的必要的资金、人员、设备、时间等是否确保	51
	2) 实施开发计划的业务分配和责任体制是否妥当	52
	3) 是否从系统整体的可靠性、安全性、有效性出发，选择机型及各种技术	55
	4) 是否作出并确认能达到系统目的并可实现的替代方案	55
	5) 开发及运行费用的核算基础是否确切	56
	6) 对效果的定性、定量评价是否确切	56
(4) 人员管理	1) 是否明确规定职务权限、不能超权	57
	2) 为了提高人员的技术水平，是否定期进行有效的教育与训练	57

2. 开发业务

项　目	内　容	说明页次
(1) 开发顺序	1) 开发顺序是否与系统开发的规模、时间以及系统特性适合	58
	2) 开发手册是否标准化以及作业内容的描述是否容易理解	58
	3) 开发手册是否随着技术的进步作相应的改进	60
(2) 人员管理	1) 是否明确规定职务权限，并禁止越权	60
	2) 是否掌握加班时间，休假时间等情况，并努力改善作业环境	61
	3) 是否定期进行有效的教育与训练，提高人员的技术水平	61
	4) 人员是否熟悉开发手册，并按开发手册进行开发	62
	5) 是否对人员进行健康检查和治疗	62

续表

项　目	内　容	说明页次
(3) 系统设计	1) 系统设计书与用户手册是否根据开发手册进行编写;是否得到负责人与用户的认可	62
	2) 系统设计书中是否记述电子计算机系统的故障对策	63
	3) 系统设计书中是否记述确保安全的各种控制手段	64
	4) 系统设计书中是否记载适当的交接计划和相应的运行计划	65
	5) 设计是否保证数据的完整性(一贯性、不变性等)	66
	6) 文件的设计书是否考虑到存取时间和存贮量可能达到的最大值	66
	7) 代码与输入输出的设计是否便于用户使用	67
	8) 数据库结构的设计与使用形式是否相符	68
	9) 数据库的存取是否有适当的控制手段	69
	10) 系统测试计划的目的、范围和时间表是否合适	69
(4) 程序设计	1) 是否按照系统设计书来设计程序说明书	70
	2) 在设计程序说明书时如产生技术或逻辑矛盾时,是否对系统设计进行再检查	71
	3) 程序说明书的标准化、模块化等是否从作业量、时间表、安全性、维护等观点考虑	71
(5) 编码	1) 是否按照程序说明书正确地编制程序	72
	2) 是否合理分配编码任务;管理者能否确切把握作业进展状况	72
	3) 程序测试结果是否完全记录下来	74
	4) 对于重要的程序是否由编制者以外的人员进行测试	74
	5) 程序文档是否按照开发手册作成	76
(6) 系统测试	1) 测试数据的作出以及测试的实施是否按测试计划进行	76
	2) 测试是否由程序编制者以外的人员进行	76
	3) 测试是否由用户参加	77
	4) 测试的结果是否得到开发部门以及用户部门负责人的认可	77
	5) 是否保管好测试结果的记录以及测试数据	77