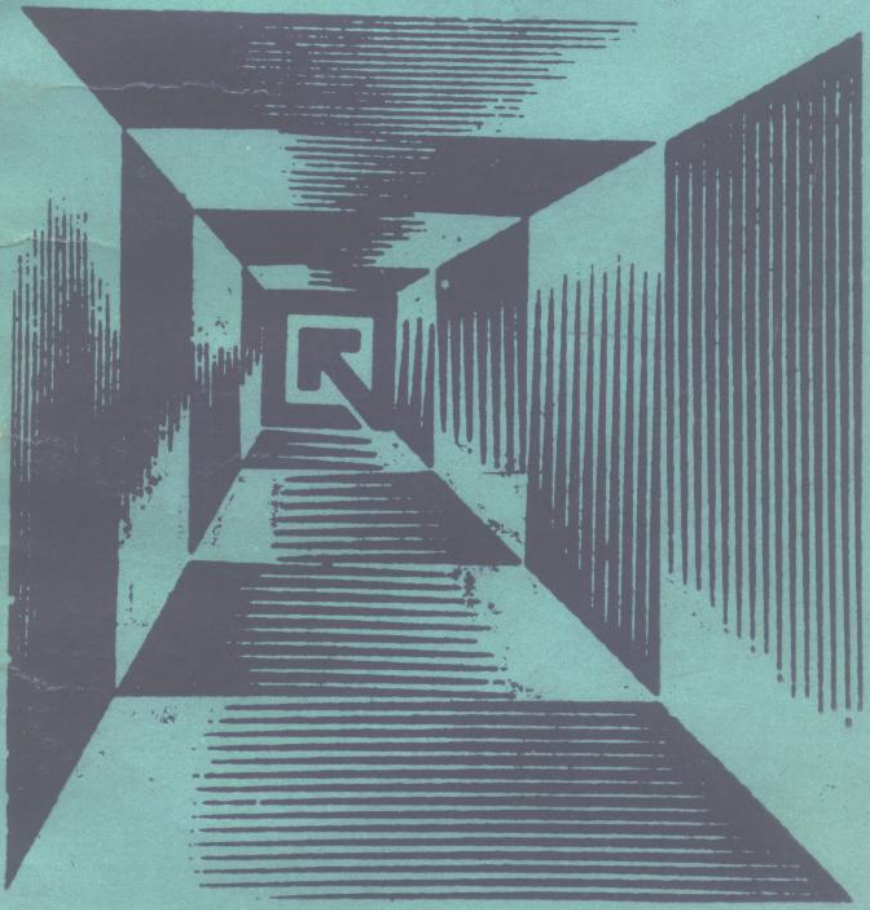
数据保护和加密研究

计算机网络的安全性

[日] 一松 信 主编



科学出版社

数据保护和加密研究

计算机网络的安全性

〔日〕一松　信　主编

史　科　译

科　学　出　版　社

1991

内 容 简 介

本书全面系统地介绍了如何在计算机网上保护数据，以及如何对数据加密脱密等问题. 全书分三章. 第一章主要讲述数据保护与密码的关系. 第二章介绍利用软件进行加密的基本技术，较详尽地叙述了DES算法、RSA算法和 MIX 算法的原理，加、脱密过程及用软件实现的方法. 第三章结合实例讲解了密码应用方面的有关事宜.

本书可供大学计算机系师生、研究生，计算机应用工程技术人员参考.

一松 信監修

データ保護と暗号化の研究

コンピュータ・ホットワークの安全性

日本経済新聞社，1983

数据保护和加密研究

计算机网络的安全性

〔日〕一松 信 主编

史 科 译

责任编辑 黄岁新

科学出版社出版

北京东黄城根北街 16 号

邮政编码：100707

中国科学院印刷厂印刷

新华书店北京发行所发行 各地新华书店经售

*

1991年11月第 一 版 开本：850×1168 /32

1991年11月第一次印刷 印张：7 1/4

印数：0 001—3 500 字数：183 000

ISBN 7-03-002385-4/TP · 176

定价：6.40 元

译 者 的 话

随着通信技术和计算机技术的飞速发展，数据传输和处理、资料联机检索等各种形式的计算机通信网络也相继发展起来，于是在比较发达的国家里，又出现了一种新的犯罪形式——计算机犯罪.一些行为不端的人利用智能打入计算机通信网络，冒领现金或窃取情报. 因此，如何保护数据就成了急待解决的问题. 本书就是适应这种形势写成的.

原书共分三章. 第一章主要讲述数据保护与密码的关系，概括地介绍了密码的历史，密码的各种形式及其优缺点；第二章较详尽地叙述了 DES 算法、RSA 算法和 MIX 算法的原理，加脱密过程及用软件实现的方法；第三章结合实例讲解了密码应用方面的有关事宜. 原书还附有 6 篇密码常识方面的短文，因与正文无直接关系，故未予译出.

本书前言和第一章由姜启魁、卜承源、金德纯、王俊雄翻译，第二章由王俊雄、曹景秀、王英才、金德纯、卜承源翻译，第三章由卜承源、陈化翻译. 姜启魁、金德纯负责全书校对.

在正式付印前，上述部分同志以及刘建军同志又对全书进行了一次复校，全书总的复校工作由金德纯负责.

由于我们水平有限，译文中定有不妥之处，欢迎广大读者予以批评指正.

译 者

1987 年 9 月

前　言

近年来，经常听到人们议论“计算机犯罪”这个问题，并且也有关于这方面的专门刊物(会员组织的)出版发行．其中提到的一些事例，大部分是由于过去对计算机管理不善和制度不健全被人钻了空子所造成的，但是，像解译通行字、伪造现金卡之类的真正属于技能型计算机犯罪的也不乏其例．

虽同属计算机犯罪，但对冒领钱财和篡改信息这一类犯罪采取相应对策并不难，而对于那些不择手段存心要破坏计算机系统，或出于一种癖好乃至有意进行智力挑战而肆意要破坏计算机的人，坦率地说，现在还没有妥善的解决办法．因此，目前的办法只能是给上述具有特异才能的人以优厚的待遇，努力把他们争取到防御这方面来．

另一方面，则要采取安全措施，以避免无意或偶然的失误酿成大事故．可以说，这对于制造和使用计算机一方来说是义不容辞的．那种动辄搬出亚森·罗平（Arséne Lupin）那个开锁的天才，认为世上没有打不开的锁，主张干脆外出不锁门的论调未免有点荒唐．而如果加上它二三道锁，这样，即使是小偷费了不少劲撬开了一道锁，也有可能灰心丧气，不再坚持干下去，也有可能在继续作案的过程中被人发现而抓住．从这个意义上讲，牢牢地加上锁，对于防止犯罪还是有用的．

对于保护计算机及其存储器中存储的信息来说也是如此，即使无法对付居心叵测的天才，也务必要考虑采取防止发生无意泄密和轻易失盗之类的防范措施．而作为一种防御手段来说，密码就是一种有效的防御手段．

一提到密码，有的人总是将它和“军事秘密”纠缠在一起，就连纯学术上的密码研究，也往往被带上有色眼镜来看待．但是，在电

气通信成为传送信息的主流的今天，仅从保护私人秘密这一角度来看，也应把密码基础知识作为一种常识让国民来了解为好．当然，密码仅是用于保护信息的一种手段，如果过份依赖它，也会发生意想不到的问题．过去已有许多计算机犯罪案例说明了这一点．

在本书出版之前，虽已有几本同类论著，但我仍为本书的问世而感到高兴．本书取材于邮政省委托编纂的“关于网络化带来的各种问题的调查研究”（数据保护技术的研究与开发）的报告．此报告无论是对国民大众还是对经济产业活动来说都很有意义．但是，考虑到这个报告专业性很强，如若原封不动地拿出来，很可能得不到社会的充分理解，加之后来又有了新的研究成果，因此，我认为若把两者归纳成一本参考书，则对于国家和国民了解上述报告宗旨将是一个好方法．

本书得以完成，应感谢邮政省的善意理解和出版社的大力协助．然而，鉴于原报告的特点，有些部分又不宜直接拿来发表，因而在本着不损害本书基本内容的前提下，对技术上的一些细节做了删节及修改，敬请谅解．

本书第一章由小野世喜彦、武井俊幸执笔，第二章由细贝康夫执笔，第三章由宫野惠执笔．细贝负责汇总，一松写了“密码花絮”．并开了几次编辑会议，为调整统一各章做了充分的研究．

在本书编著过程中，由于主编去中国出差，给各位执笔者添了诸多麻烦，谨请谅解．

值此书出版之际，谨向给予大力协助与支持的邮政省宇宙通信企画课课长江川晃正先生（前任数据通信课课长）、数据通信课课长内海善雄先生及联合系统开发股份有限公司前任常务董事高田希一先生深表谢意；谨向为本书写了推荐词的邮政省电气通信政策局局长小山森也先生表示衷心感谢；最后向从酝酿著书到出版都不断给予鼓励和支持的日本经济新闻社出版局第一编辑部次长神山直树先生深致谢意．

一松　信

1983年6月

目　录

第一章　数据保护与密码

一、信息社会与数据通信

1. 推进信息化的数据通信

(1) 信息化和数据通信

“现在，我们正生活在一个信息社会”，此说已有时日，然而若真的坐下来问问自己：“何谓信息社会?” 竟难以作答。现在可能很少会有人对“信息”这个词感到陌生，因此，或许可以这样回答，所谓信息社会，从某种意义上讲，就是“信息化”崭露头角，即信息处于领先地位的社会。

在《现代用语基础知识》(自由国民社出版)中，对信息社会作了如下定义：“信息社会是以生产信息价值为中心使社会和经济向前发展的社会，在这个社会里，信息成为比物质和能源更加有用的资源。”即：可以把信息的检索、传送、存储、处理、控制等变为社会和经济活动重要因素的社会叫做信息社会，而把这种趋势的进一步发展叫做信息化。

确实，在今天，我们必须承认在信息这个无形物中所存在的价值。这几乎是不可抗拒的。以前我国常有人说信息是不能卖钱的。然而大量登载电影、戏剧、文艺演出等消息的街头信息小报却颇有销路；有一家公司每周都通过计算机系统源源不断地向人们提供选择配偶的数据，历时已经两年，申请加入的人仍然络绎不绝。由此可见，信息不能卖钱之说现在已经根本没有市场了。

社会信息化的进展与通信和计算机的发展有着密不可分的关系。由于通信和计算机有了迅猛发展，上述的信息检索、传送、存储、处理、控制等都实现了高速度和高效率，从而大大地克服了时间和距离上的障碍，使信息的价值飞速提高，从而使社会的信息化

得到进一步发展。

通信和计算机相结合就是数据通信。也就是说，数据通信是将信息传送及信息处理作为一个整体来进行的通信，它是通过把计算机接到通信线路上来实现的。数据通信在时间上、距离上给信息增添了基本价值，同时又能通过信息的比较、综合、交流等产生新的附加价值。

用来进行数据通信的系统即数据通信系统是由计算机、通信线路、终端等构成的。人们熟悉的国铁绿色窗口和银行、邮局等的存款、汇兑联机系统就是典型的数据通信系统。通过它们，我们在全国任何一个地方都可以随时订到车票或存取现金等，从而能够享受数据通信带来的很多方便和恩惠。

迄今为止，社会的信息化一直是以无线电广播、电视广播这类广播系统等手段为中心的。最近，由于出现了数据通信、传真通信等新的通信手段，社会信息化的进展更快了。例如，联机数据库的利用正在发展，它使得对于学术信息及报道信息等的检索实现系统化成为可能。另外，利用电视接收机和电话网的文字图形信息网络系统便能根据用户要求在电视上播出文字和图形等多种信息。这种系统一经开业(预计在 1984 年)，即便在家里也能及时地得到所需信息，从而可以进一步享受信息化社会的恩典。

国内数据通信系统的数量增长情况如表 1-1 所示，从中可以看出近几年的平均年增长率为 30%。按照这个速度发展下去的话，数据通信必将对社会信息化做出更大的贡献。

(2) 数据通信的高级化

现在这个时代是讲究战略战术的时代。战略战术存在的意义就在于以最小的付出获取最大的效益，这对私人企业来说，就是以最小的投资赢得最大的利润；对公共企业和政府来说，就是既要花费最少又要最大限度地实现其本来的目的(如公共福利事业、保障基本人权等)。此外，有军事实力的国家拥有多大规模的军备才能对假想敌国构成有效的遏制力量，也就是说，拥有多大规模的军备

表 1-1　日本国内数据通信系统年度设置情况

区别＼年度		44	45	46	47	48	49	50	51	52	53	54	55	56
系统数	自营系统	122	188	295	441	706	1,126	1,429	1,999	2,689	3,403	4,598	5,807	7,095
	公社系统	4	7	13	27	38	42	50	58	60	65	70	72	76
	合计	126	195	308	468	744	1,168	1,479	2,057	2,749	3,468	4,668	5,879	7,171
	对上年度增加数	49	69	113	160	276	424	311	578	692	719	1,200	1,211	1,292
与上年度比(%)		164	155	158	152	159	157	127	139	134	126	135	126	122

注：自营系统系指国营公司系统以外的系统．国营公司系统就是日本电电公司设置的系统．

摘自邮政省 1982 年版《通信白皮书》．

才能保证本国的安全，这也是战略战术要研究的课题．

在运用战略战术中，如何搜集有用信息，以及如何处理这些信息才有助于制定计划是基本课题．要搜集信息，利用通信是最有效的．如果能利用全世界的通信网络，那么不用出门就能在短时间里搞到来自世界各地的宝贵信息．早在 19 世纪就曾有人说“海底电缆胜于战舰”．据说维多利亚时代英国占优势的原因之一就在于它拥有一个世界情报网．其次，要处理搜集来的信息并决定如何使用它，最好是借助于计算机．把搜集到的信息按一定规则分类整理是计算机的拿手本领，要迅速正确地做出判断，则计算机是必不可少的工具．

这样看来，要有效地运用战略战术，就必须借助于电信和计算机，也就是说信息传送与信息处理融为一体的数据通信应该出世．不言而喻，这种场合的数据通信系统与其独立存在，莫如相互连接（数据通信的高级化）组成大规模网络，这样，其价值就会更高．

数据通信的意义归纳起来有如下几点：①提高社会和经济活动的效率，为国民生活提供更多的方便和提高科学文化水平做出很大贡献；②能够促进人们在社会和经济活动中节省人力和能源；③它涉及的领域非常广泛，其中有与通信有关的产业、计算机

产业、软件产业等，而且它本身就是有很高附加价值的知识密集型产业，人们对它寄予很大希望；④从国家利益上讲，为了处理作为社会和经济活动基础的信息，也需重视数据通信，等等．综上所述，既然数据通信有如此重要的意义，人们当然就希望发展它，使其向高级化方向发展，并把它作为一个重要课题来研究．

数据通信高级化，一般也可以说成是计算机或数据通信系统的网络化．即如图 1-1 所示，利用通信线路把单独使用的计算机和独立使用的数据通信系统连接起来，整个构成一个有机的网络（计算机网络），这样就能实现数据通信的高级化．实现网络化可

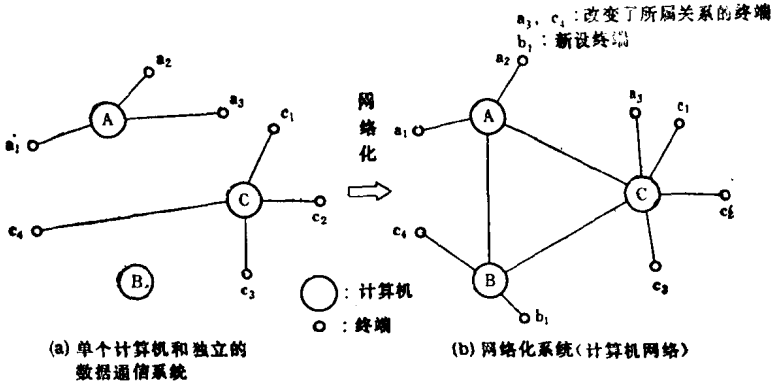


图 1-1　计算机与数据通信系统的网络化

能带来的好处归纳起来有如下几点：

① 促进行政机构、地方团体、企业、个人等相互间进行顺利而密切的交流，形成一个富有活力的信息化社会．

② 在高度发达的网络系统中，不管在什么地方，也不管是谁都能用简易的通用终端通过网络得到丰富多彩的服务．

③ 通过纠正由于信息量的增大而带来的在信息利用方面的地区间差距和企业间差距，以保持均等利用信息．

④ 通过发展医疗、教育等与社会生活有密切关系的各种系统，使社会生活既安全又丰富．

⑤ 通过共同利用构成数据通信系统的通信线路、硬件（计算

机、终端等)、软件(计算机程序)、数据库(计算机存储的信息)等各种资源,能够避免重复投资,减少开发和使用费用,缩短开发时间,促进资源的有效利用.

⑥ 由于可以通过网络进行相互联系、召开会议以及进行其他业务活动,故不必再使用交通工具了,从而会更加促进在社会和经济活动中节省人力和资源.

1982年秋,数据通信线路在使用上实行了第二次自由化,使线路的使用和连接方式获得了更大的自由,并允许计算机相互连接.因此,网络化的发展形势空前高涨.那么,具体说来有哪些方面需要网络化呢?

第一是一般企业.在信息处理对企业来说是生死攸关的信息化社会里,高效率地搜集、分析和处理信息,提高为顾客服务的水平,灵活运用市场战略和经营战略,正确地下定决心,这些都是必不可少的.为此,不仅在本企业内,而且在企业集团内的各公司之间,进而在贸易企业或同种企业之间都有谋求系统网络化的动向.

市场战略中有后方一体化,前方一体化和同业一体化之说[1].所谓后方一体化是指企业以加强向本企业提供资源的厂商的控制来保证企业发展;前方一体化是指以加强与本企业商品、业务有关的流通部门的控制来保证企业发展;同业一体化是指以加强与本企业竞争对手的控制来保证企业发展.所说的加强控制是指买下它的企业或作它的大股东.

例如制造汽车的企业把增长率高、利润大的制造汽车零件的企业并为子公司,这就是后方一体化;反之,如果掌握了汽车销售公司的实权就是前方一体化.另外,在不形成个人垄断的前提下买下竞争企业,这就是同业一体化.但是,判断是否要把这些战略付诸实施,关键是要有准确的信息和正确的判断,并且,高效率疏通企业之间的信息会进一步提高一体化的效果,因此需要一个网络化系统.

第二是行政部门需要网络化.目前对行政工作普遍要求提高效率和简化手续,这就要求通过引进数据通信系统和实现系统网

络化来推进高效率和合理化，这也是时代的潮流。另外，预料在行政机关和民间企业之间也将实行网络化，以便利用行政信息或自动支付税金和保险费[2]。

第三是与生活有关的系统需要合并。预料今后教育、医疗、环境、防灾等社会生活方面的系统的需要将会进一步增长，类似的系统将在全国各地设置起来。因此需要有公用数据库、公用软硬件及在系统间相互交换信息，由此可以推测今后各地对系统网络化的需求将会出现一个高潮[2]。

(3) 数据通信的前景

前面已经讲到，数据通信由于实行网络化而将进一步向高级发展，那么，将来的高级计算机网络将是个什么样子呢？图 1-2 所示的网络应用的基本构想可作为它的一个答案[2]。

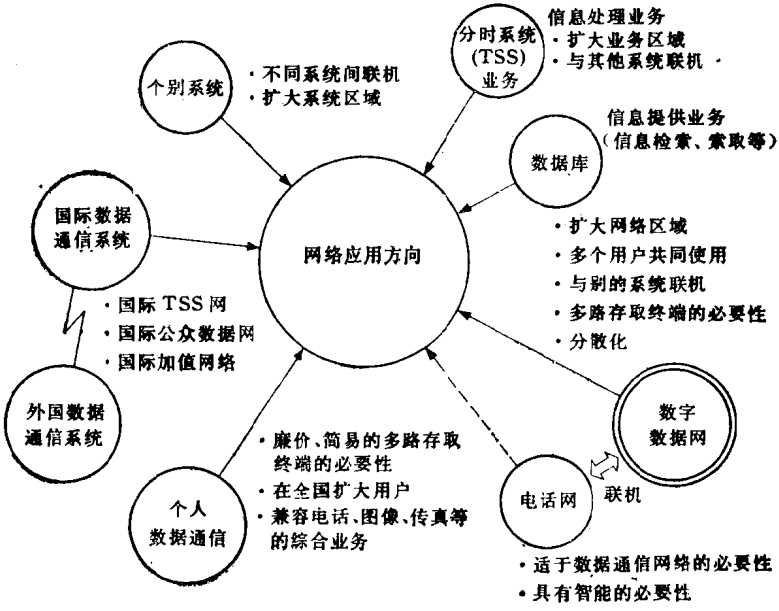


图 1-2 网络应用的基本构想

——摘自《商业通讯》1978 年 2 月号