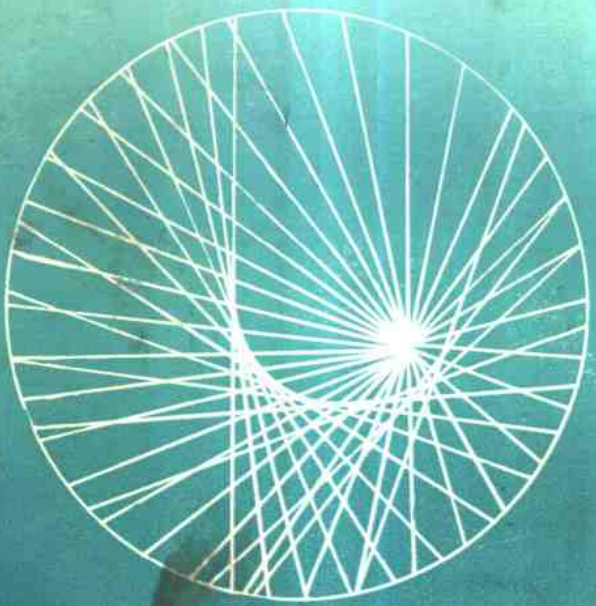
数据保护与加密

计算机网络的安全性

一松 信 主编　周保太 译　于德中 校



西南师范大学出版社

数据保护与加密

——计算机网络的安全性

一松　信　主编

周保太　译

于德中　校

西南师范大学出版社

数据保护与加密

一松 信　主编

西南师范大学出版社出版
（重庆 北碚）
新华书店重庆发行所经销
重庆九宫庙印刷厂印刷

开本：787×1092 1/32 印张：8.5 插图：2 字数：181千
1990年4月第一版　1990年4月第一次印刷
印数：1—1,000

ISBN 7-5621-0363-1/O·29
定价：2.70

译　序

近年来，随着计算机技术的广泛应用，计算机通信网络也得到了迅速的发展，因而数据安全保密问题成了人们十分关注的问题。为了满足目前国内有关单位和广大读者了解和掌握数据安全保密的理论原理和方法的迫切需要，现翻译了日本著名密码学专家一松　信主编的《数据保护与加密——计算机网络的安全性》（データ保护と暗号化の研究——コンピュータ・ネットワークの安全性）一书。

本书是一部系统论述计算机网络的数据保护和加密的专著，详细介绍了数据加密标准、公开密钥密码体制和混合加密体制的具体实施方案。

该书内容新颖，通俗易懂，图文并茂，面向普及。是党政机关、大专院校、研究单位从事计算机网络保密系统的设计人员和管理人员必备的工具书和参考书，也是业余爱好者难得的一本教材。

本书在翻译出版过程中得到了孙玉久同志的帮助，在此表示感谢。

译　者

一九八八年十二月

编者的话

近年来，常听到“计算机犯罪”这种说法，也出版了专门刊载这方面内容的杂志。大部分似乎都是介绍利用计算机管理和制度上的漏洞而施展计谋，进行破坏的例子；也有破译通行字，伪造现金卡这种真正计算机犯罪的事例。

即使在计算机犯罪方面，对于侵吞财物和篡改信息这类犯罪还容易采取措施，但对于作为一种兴趣乃至智力挑战而立志破坏计算机者，直率地讲，目前还没有有效的防范措施。最佳的对策是，给予这方面有特殊才能的人以优厚的待遇，力争把他们吸引到防御者一边来。

另一方面，对于制造和使用计算机的人来说，义不容辞的责任是采取安全措施，以避免因偶然因素或不小心而酿成大事故。有人说，如果遇到ARSE\NE LUPIN（法国一个非常有名的大盗——译者注）那种什么锁都能打开的天才，最好是家里没人时不锁门。这种说法纯属谬论。如果上二道锁、三道锁，要费尽心血破开一道锁的小偷，也会因厌烦而死心，或者容易在耗费时间的过程中被人发现而遭逮捕。从这种意义上来说，牢固地锁好门，对防止犯罪是有益处的。

保护存贮在计算机和存贮设备中的信息也同样如此。对于居心不良的人，即使不能与之抗衡，也一定要设法采取安全防御措施，以免信息因不注意而泄露或转眼被盗。其手段之一就是使用密码。

谈起密码，人们往往把它同军事机密联系在一起，即使纯学术的密码研究，也常被蒙上一层神密的色彩。但是，在

电信传递信息已成为主流的今天，即使从私人保密的角度来看，密码的基础知识也应成为国民的常识。当然，密码不过是保护信息的一种手段。意想不到的事故，大量的计算机犯罪案例，都暗示人们一定要使用密码。

以前也出版过几本这方面的书籍。这次出版该书，本人感到由衷的高兴。本书的素材来源于受邮政省委托编写的《网络化中诸问题的调查研究》（数据保护手段的研究和开发）。该调查研究无论是对个人，还是对经济活动都是非常有意义的。由于它的专业知识较深，照原样发表很难被社会上的一般人所理解，同时在此之后情况又有了新的变化，因此把这些材料综合在一起，汇编成参考书，这样无论是对国家，还是对国民都是一个上策。

承蒙邮政省的支持，出版社的协助，本书才能够出版。但是，有些地方很难照原样发表，在不影响本书实质性内容的前提下，对某些技术上的细节作了省略或修改。

本书的第一章由小野喜世彦和武井俊幸执笔，第二章由细贝康夫执笔，第三章由宫野惠执笔，全书由细贝康夫进行汇总，并召开了多次编辑会议，充分注意了各章的统一。

由于主编出访中国，给各位执笔者增添了不少麻烦。在此对出版给予大力帮助和指导的邮政省宇宙通信规划课课长江川晃正先生（前数据通信课课长）、数据通信课课长内海善雄先生、系统开发股份公司前常务董事商田希一先生深致谢意，并衷心感谢邮政省电信政策局局长小山森野先生的大力推荐。最后还要对从计划到出版给予不断鼓励和帮助的日本经济新闻社出版局编辑部副部长神山宣树先生深致谢意。

1983年6月　　一松　信

目　录

第一章　数据保护与密码……（1）

第一节　信息化社会与数据通信……（1）

一、　加速信息化进程的数据通信……（1）

1．　信息化与数据通信……（1）

2．　数据通信网络化……（4）

3．　未来的数据通信……（7）

二、　数据通信信息化的障碍……（8）

1．　数据通信网络化的前景和问题……（8）

2．　促进信息化健全地发展……（11）

第二节　数据通信网络中的数据保护措施……（12）

一、　数据保护的着眼点……（12）

1．　数据保护的有关问题……（12）

（1）私人秘密保护/（2）确保安全/（3）提高可靠性

2．　对网络的威胁……（17）

3．　保护措施……（19）

二、　网络的数据保护措施……（20）

1．　主机和终端的数据保护措施……（20）

2．　通信网上的数据保护措施……（23）

3．　全网络的数据保护措施……（23）

第三节　用密码保护数据……（24）

一、　密码的目的和用途……（24）

1．密码的目的……（24）
2．密码通信……（25）
3．密码的功能……（27）
（1）保护传输的数据/（2）保护存贮的数据/（3）验证通信对方
4．使用范围……（29）
二、密码的基本方式……（30）
1．密码分类……（30）
2．密码简史……（32）
3．密码的基本方式……（35）
（1）编码方式和密码方式——加密单位/（2）序列密码和分组密码/（3）代替式、置换式和插入式密码/（4）密码的安全性——绝对安全性和计算量的安全性
第四节 密码体制概述……（37）
一、传统密码体制……（37）
1．采用传统密码体制进行通信……（37）
2．DES算法……（39）
3．传统密码体制的密钥管理……（41）
二、公开密钥密码体制……（43）
1．采用公开密钥密码体制进行通信……（44）
2．数字签名……（45）
3．RSA算法……（47）
4．公开密钥密码体制的密钥管理……（49）
三、采用MIX方式的密码体制……（50）
1．传统密码体制和公开密钥密码体制的优点和缺点……（51）
2．采用MIX方式进行通信……（54）
参考文献……（55）

第二章　利用软件加密的基本技术……(58)
第一节　密码系统的功能、目标和范围……（58）
1．把密码系统引入通信系统的方法……（58）
（1）链路加密方式/（2）节点加密方式/（3）端对端加密方式
2．密码体制分类……（60）
（1）传统密码体制/（2）公开密钥密码体制/（3）采用混合方式的密码体制
3．密钥管理体制……（61）
4．密码系统的保护对象和范围……（61）
（1）通信保护/（2）文件保护
第二节　传统密码体制的基本加密技术……（63）
一、DES算法的实现……（63）
1．DES的雏形……（63）
2．DES算法……（68）
(1)加密处理/（2）脱密处理/（3）加密变换F(R,K)/（4）密钥安排
二、DES方式的密码强度分析……（80）
1．对蛮干攻击法的讨论……（81）
2．对密文统计结构的讨论……（81）
三、DES方式的基本设计……（82）
1．DES方式密码处理概要……（82）
2．DES方式的功能概要……（83）
（1）密钥构成/（2）密钥管理模型/（3）密码子程序/（4）密钥的编制和存贮/（5）密钥分配/（6）数据加密和脱密/（7）DES方式的功能小结
3．DES方式的软件设计……（118）

第三节　公开密钥密码体制的基本加密技术……（120）
一、　RSA 算法的实 现……（120）
1．　加密和脱密方法……（120）
2．　RSA 算法的数学根据……（121）
3．　RSA 算法的实现……（122）
（1）加密和脱密处理/（2）产生和判定大素数的方法/
（3）d的选择方法/（4）由 φ(n)和d计算e的方法
4．　简单举例……（126）
二、　数字签名……（127）
三、　RSA方式的密码强度分析……（133）
1．　模参数n的位数……（133）
2．　探索素因子分解以外的脱密参数的方法……（133）
3．　设置参数p、q、e，d的条件……（134）
四、　RSA方式的基本设计……（136）
1．　RSA方式的密码处理概要……（136）
（1）公开密钥和秘密密钥的保存/（2）密码数据通信
2．　RSA 方式的功能概要……（137）
（1）密钥结构/（2）密钥管理模型/（3）密码子程序/
（4）编制和存贮密钥/（5）密钥分配/（6）数据加密和
脱密/（7）报文验证/（8）RSA方式功能小结
3．　RSA方式的软件设计……（147）
第四节　采用MIX方式加密的基本技术……（154）
一、　MIX方式的目标……（154）
1．　DES 方式和RSA方式的优点与缺点……（154）
（1）密钥管理/（2）安全性/（3）实用性
2．　MIX 方式的目标和优点……（155）
二、　MIX方式的基本设计……（156）
1．　MIX方式的密码处理概要……（156）

2． MIX 方式的功能概要 ……（157）

（1）密钥结构/（2）密钥管理模型/(3)密码子程序/（4）密钥的编制和存贮/（5）密钥分配/（6）数据加密和脱密/（7）MIX方式的功能小结

参考文献 ……（166）

第三章 密码的应用技术……（168）

第一节 密码的应用方法……（168）

一、 密码的任务……（168）

二、 密码的引入方式……（169）

1． 引入方式……（169）

（1）链路加密方式/（2）节点加密方式/（3）端对端加密方式

2． 网络和端对端加密方式……（171）

3． 密码和网络结构……（171）

4． 密码和通信功能……（173）

（1）传送控制程序/（2）基本属性处理

三、 密码协议……（175）

1． 密钥设置……（175）

（1）DES方式密钥的结构和设置/（2）RSA方式密钥的结构和设置/（3）MIX方式密钥的结构和设置

2． 密钥分配……（177）

3． 数据加密和脱密……（179）

（1）DES方式/（2）RSA方式

4． 报文验证……（182）

第二节 密码处理方法……（184）

一、 密钥的设置和处理……（184）

1. DES方式密钥的设置和处理……（184）
（1）主机主密钥的设置/（2）终端主密钥的设置/
（3）密钥加密密钥的设置（4）密钥的更换
2. RSA方式的密钥设置和处理 ……（187）
（1）秘密密钥和公开密钥的设置/（2）密钥更新
3. MIX方式的密钥设置和处理 ……（189）
二、 密码通信处理……（190）
1. DES方式的密码通信处理 ……（191）
（1）发方主机的处理方法（向终端发报）/（2）收方
终端的处理方法/（3）发方主机的处理方法（向主机
发报）/（4）收方主机的处理方法
2. RSA方式的密码通信处理……（199）
（1）发方节点的处理方法/（2）收方节点的密码处理方法
3. MIX方式的密码通信处理 ……（204）
（1）发方节点的处理方法/（2）收方节点的处理方法
4. 数字签名和译码签名 ……（208）
（1）发方节点/（2）收方节点
第三节 设计一个密码系统……（209）
一、 密码系统的设计概要……（209）
1. 密码系统的范围和前提 ……（210）
（1）基本范围和前提/（2）软件的编制方针
2. 密钥管理应用程序概要 ……（211）
3. 密码子程序概要 ……（212）
4. 程序结构 ……（215）
5. 功能与规格 ……（219）
6. 编制程序时应注意的事项 ……（230）
二、 DES方式的基本试验……（230）
1. DES算法 ……（230）
2. 密钥管理 ……（233）

3． 数据加密……（235）
三、 RSA 方式的基本试验……（237）
1． RSA 算法……（237）
2． 密钥管理……（237）
3． 数据加密……（238）
四、 在网络中进行密码通信试验……（242）
1． 由终端向主机进行密码通信……（242）
2． 由主机向终端进行密码通信……（245）
3． 主机之间的密码通信……（245）
五、 密码系统应用举例……（247）
1． 模型系统概要……（248）
(1)付款通知数据和付款表／(2)系统功能／(3)引入密码系统
2． 程序结构和密码方式……（249）
3． 系统操作和程序处理……（251）
4． 加密举例……（254）
参考文献……（255）

第一章　数据保护与密码

第一节　信息化社会与数据通信

一、加速信息化进程的数据通信

1．信息化与数据通信

人们早就说，“我们现在是生活在信息化社会里”。但若郑重其事地自问自答一下“什么叫信息化社会？”就感到非常困难。所谓信息化社会，在某种意义上可以说是信息先行的社会。

如果按照《现代用语基础知识》（自由国民社版）的解释，信息社会应定义为“信息成为比产品和能源价值更高的资源，以生产信息价值为中心，并推动社会和经济向前发展的社会。”即以信息检索、传递、存贮、处理和控制等构成社会和经济活动重要成份的社会称为信息化社会，更进一步发展，就可以叫作信息化。

的确，今天我们都必须承认信息这个无形之物的价值。直到最近人们还常说，信息是不能卖钱的。但是，大量刊登电影、戏剧等消息的杂志在销售，婚姻介绍公司用计算机系统每周提供适合结婚的对象数据，人们纷至沓来，请求加入这样的公司。这一切使人感到那种信息不值钱的说法马上就要过时了。

另一方面，社会信息化的发展与电信和计算机的发展有着密不可分的关系。电信和计算机的发展，可以高速有效地对信息进行检索、传递、存贮和控制，从而克服了时间和空间的制约，使信息的价值得到了飞跃的提高，大大加速了社会信息化的进程。

把电信和计算机结合起来，就是数据通信。所谓数据通信，就是用电信线路把计算机等连接起来，把信息传递和信息处理作为一个整体进行的通信。数据通信既为信息付出了时间和距离的基本代价，又从信息的比较、结合和交流过程中生产出新的价值。

执行数据通信的系统，即数据通信系统，由计算机、通信线路和终端等构成。众所周知的国营铁路绿色窗口，银行、邮局等的存款、汇兑联机系统就是采用数据通信系统。采用这些系统，我们就能够随时在全国任何地方预订座位，或者在全国任一地方存款和取款，享受数据通信系统带来的方便和好处。

社会信息化，以前是以无线电和电视广播这种大型设备为中心发展的。最近采用数据通信、传真通信等新的通信设备，进一步加快了其发展速度。例如，用联机数据库检索学术情报、消息报导等。还有，如果使用电视接收机和电话网，CAPTAIN 系统可根据用户要求，把各种信息以文字和图象的形式放映在电视上，为您提供服务，坐在家里就能及时得到您所需要的各种信息，进一步享受信息化社会的好处。

表 1 示出了国内数据通信系统的变化情况。其年增长率大约是30%左右。如果继续以这样的速度增长下去，数据通信就会为社会的信息化作出更大的贡献。

表1—1　日本各年度数据通信系统的设置状况

分类 \ 年度		1969	1970	1971	1972	1973	1974	1975	1976	1977	1978	1979	1980	1981
系统数量	独资经营系统	122	188	295	441	706	1126	1429	1999	2689	3403	4598	5807	7095
	公司系统	4	7	13	27	38	42	50	58	60	65	70	72	76
	合　计	126	195	308	468	744	1168	1479	2057	2749	3468	4668	5879	7171
	比上年度的增加数	49	69	113	160	276	424	311	578	692	719	1200	1211	1292
	与上年度的比率(%)	164	155	158	152	159	157	127	139	134	126	135	126	122

注：独资经营系统＝公司以外的系统

公司系统＝日本电报电话公司设置的系统

出处：通信白皮书，邮政省1982年版

2. 数据通信网络化

现代是战略和战术的时代。战略和战术存在的意义就在于用最小的努力获得最大的成果。在私人企业内，就是用最少的投资获得最大的利益；在国营企业或政府中，就是尽可能用最少的费用实现其原来的目的。另外，具有军事力量的国家的战略和战术目标是：具备何种程度的军备，才能对假想的敌国进行有效遏制，确保本国的安全。

战略和战术的基本课题是：如何收集有效的情报，怎样对它进行处理，才能对制订计划有用。用电信收集情报最有效。如果能够利用全世界的电信网，坐在家里就可以在极短的时间内获取世界各地的重要情报。即使在十九世纪，就已有“海底电缆战胜敌舰”的说法。据说英国在维多利亚时期占居优势的原因之一就是掌握了世界的情报网。处理收集的情报的最佳办法是借助于计算机的力量。计算机可以得心应手地把收集的情报按一定的规则分类、整理；它是正确而迅速作出判断的不可缺少的工具。

如果这样理解的话，要想有效地运用战略战术，就必须借助于电信和计算机。即，实现把信息传递和信息处理融为一体的数据通信方式。当然，与其数据通信系统单独存在，不如互相连结成为一个大网络的价值更高。

数据通信的意义在于：①提高了社会和经济活动效率，方便了人民生活，提高了科学文化水平。②可以促进社会、经济活动，作到省力、省能。③支持了与通信有关的工业、计算机工业、软件工业等部门的发展，也促进了高知识密集产业的发展。④由于处理构成社会和经济活动基础的信息，