ISSN 0910-6707

1987

# Japan Computer Quarterly

Formerly JIPDEC Report

Japan Information Processing
Development Center

## Systems Security
## —The Fight Against Computer Crime—

No. 71

# Japan Computer Quarterly

## 1987

*Japan Computer Quarterly* (JCQ) is published quarterly by the Japan Information Processing Development Center (JIPDEC), Kikai Shinko Kaikan Bldg., 5-8 Shibakoen 3-chome, Minato-ku, Tokyo 105 Japan.
Publisher: Eiji Kageyama, President
Editor: Yuji Yamadori, Director Research & International Affairs

JIPDEC is a non-profit organization founded in 1967 with the support of the Ministry of International Trade and Industry, the Ministry of Posts and Telecommunications and related industry circles for the purpose of promoting information processing and the information processing industry in Japan.

JCQ, formerly called the *JIPDEC Report*, was first published in September, 1970 and is prepared with the assistance of the Japan Keirin Association through its Machine Industry Promotion Funds.



Translated by John McWilliams
Printed by Seibunsha Co., Ltd.
Printed in Japan, October, 1987

## CONTENTS



**No. 71**

# FROM THE EDITOR

Technological innovations and expanding applications are making computers as indispensable to everyday life and living as they have become to the world of industry and business. In particular, computer utilization in the form of online systems interconnected via telecom lines is spreading rapidly in line with the appearance of various types of personal computers, workstations and other terminal equipment. The third wave of online system construction is already being undertaken in Japan by city banks and other organizations, ushering in the age of teleshopping and telebanking.

However, this expansion and diversification of computer usage has brought with it an increase in system malfunctions and other trouble, not all of which is accidental. Computer systems are providing criminals with a new dimension for illegal activities. The more complicated the configuration of a computer system is, the more opportunities it provides for criminal acts. The overwhelming majority of such computer crimes do not result in physical damage to the computer systems themselves. Rather, these crimes are directed against what is in these systems, their contents. As such, computer crimes not only result in losses to the companies that operate these systems, but have a great influence on society as well. Japan is steadily moving in the direction of a card-based cashless society. Compared to the United States and Europe, however, Japanese people still rely quite heavily on cash as their medium of exchange. It's not surprising to find out then that computer crimes in Japan involving cash dispensers (CDs) are numerous. During the past year, in fact, nearly 1,000 CD-related computer crimes were reported here.

Various measures designed to prevent these kinds of crimes have been devised to date. But everytime a new safeguard is employed, computer criminals are quick to ferret out its vulnerabilities. It is a vicious circle, with those people determined to prevent computer crime pitted against computer criminals in a never-ending race. Looked at in this light, there is no such thing as a security measure capable of completely preventing criminal acts committed intentionally.

Be they accidental malfunctions or intentional criminal acts, preventing computer system troubles requires huge outlays of funds; and investments in system security do not increase produc-

tivity. For this reason, there are many computer system users in Japan who prefer to bear some losses due to system trouble than to shell out the large sums of money needed to protect their systems against malfunctions and/or computer crime. This situation itself tends to invite criminal acts.

Legislation related to computer crimes has been extremely slow getting started in Japan. In fact, it wasn't until just this year that the Japanese penal code was partially revised to deal with certain types of computer crimes. These amendments went into effect in June, 1987. However, this revised legislation does not cover the illegal acquisition of computer data and/or programs; the unauthorized utilization of computer systems; or the intervention into a systems operation. Under these circumstances, Japan is obligated to take a good close look at computer crime and the measures necessary to prevent it. One big drawback to this is the fact that computer specialists are unaquainted with the law, and legal specialists are not computer specialists.

Japanese people have a tendency to play up the positive aspects of computers and computer systems, such as technical innovations and the development of new products, and to give high priority to corporate strategies. However, when it comes to standardization and the revision of legal and other related systems, i.e. the "negative aspects" of this field, we tend to pay little attention. It is only natural that the positive aspects of computer systems are attractive to service vendors, but if we hope to promote the development of a sound information society, we cannot afford to overlook the less positive aspects of these systems.

Systems audits are one means of preventing computer crimes while ensuring the efficiency, reliability and security of computer systems. Steps designed to perfect systems auditing systems and to cultivate systems auditors are priority items in Japan. The Ministry of International Trade and Industry has already devised systems auditing criteria, and has implemented an examination designed to evaluate systems auditors.

In the midst of the rapid progress of informatization, Japan is striving to improve the legislative aspects of computer systems in line with advances in information technology in hopes of achieving a well-balanced information society.

Yuji Yamadori
Director
Research & International Affairs

# COMPUTER SECURITY: REQUIREMENTS AND MEASURES

Takao Nakayama
Managing Director
Center for the Informatization of Industry
JIPDEC

## INTRODUCTION

Security measures for computer systems have grown more complex and advanced in line with the recent spread of online systems. Whereas computer security and telecommunications security used to be handled separately, the widespread use of online systems has made it necessary to merge the two together.

Telecommunications are governed by the Electric Communications Law, which regulates safety measures pertaining to switching equipment, transmission lines and related facilities, and protects the secrecy of communications during transmission. Telecommunications security also benefits from 100 years of accumulated knowhow in the formulation of measures designed to protect telecommunications facilities against earthquakes, lightening, typhoons and fires.

Computer systems security adheres to security criteria formulated to protect computer centers and related facilities. Computer centers are certified and ranked according to the extent to which they implement these criteria. Computer system security measures are steadily being introduced into computer center operations industrywide.

The appearance of online systems interconnecting general-purpose computers via telecommunication lines resulted in the fusion of telecommunications and data processing. Now, whenever there is a malfunction in telecommunications hardware or software, the data processing element of the system must also be shut down, and vice versa. Security measures related to both the telecom and data processing functions of online systems must therefore be devised synergistically.

Telecommunications systems are often referred to as the nervous system of a nation, and as such, security measures related to telecom facilities and the protection of secrets transmitted via telecom systems are considered extremely important. Breakdowns in communications have always had strong impacts on society. However, the recent fusion of telecom and data processing capabilities means that today breakdowns in telecommunications also involve a loss of data processing capabilities, a factor that makes the impact of systems downtime even greater.

## ONLINE SYSTEMS SECURITY

### Networking

Interconnecting computer systems via telecom lines enables the resulting online systems to be extended nationally and even internationally. For example, the Society for Worldwide Interbank Financial Telecommunications (SWIFT) has developed a system that links hundreds of banks from around the world together via telecom lines. Then there is the aeronautical management system provided by the Societe International de Telecommunications Aeronautiques (SITA) which interconnects 248 airline companies from 154 different countries worldwide using international telecom lines. There are also nationwide and international ordering and delivery network systems in the distribution industry that interconnect major manufacturing firms with their subsidiaries, client warehouses, wholesalers and transportation firms.

When computer systems are first introduced into companies they are generally used in the batch mode. Batch systems are confined to specific locations, which means that if the operators of those systems secure the buildings that house the computers and practice strict access control they can prevent computer crime and system malfunctions. However, computer systems are like living things in that as companies use them, they tend to grow and evolve. Computers initially installed for use as batch systems eventually evolve into online systems. Since data entered into batch systems is gathered together in the form of vouchers and other documents mailed to the operators of these systems, totalling and analysis operations performed on this information tend as a rule to be slow. For this reason, firms in the extremely competitive distribution, banking and transportation fields opted for online systems as a means of staying ahead of the competition. Those firms that create in-house online networks find that this approach does not afford them the efficiency and productivity they seek, and sooner or later they decide to construct jointly-operated online systems interconnecting them with their subsidiaries, subcontractors and clients.

Figure 1 illustrates this process, showing how an in-house batch system evolves into an in-house online system, and from there to a vertical online system interconnecting the various members of a corporate group. In an attempt to keep pace and remain competitive with the huge corporations and their jointly-operated vertical online systems, small- and medium-sized firms within a certain industry or co-located in a specific region or area, cooperate with one another to construct jointly-operated horizontal online systems. There are those firms who take this process one more step by interconnecting their systems with even larger networks, such as telephone or telegraph networks, facsimile networks, cable television, and telecomputing networks, to put computer terminals onto the desks of individual employees at small-

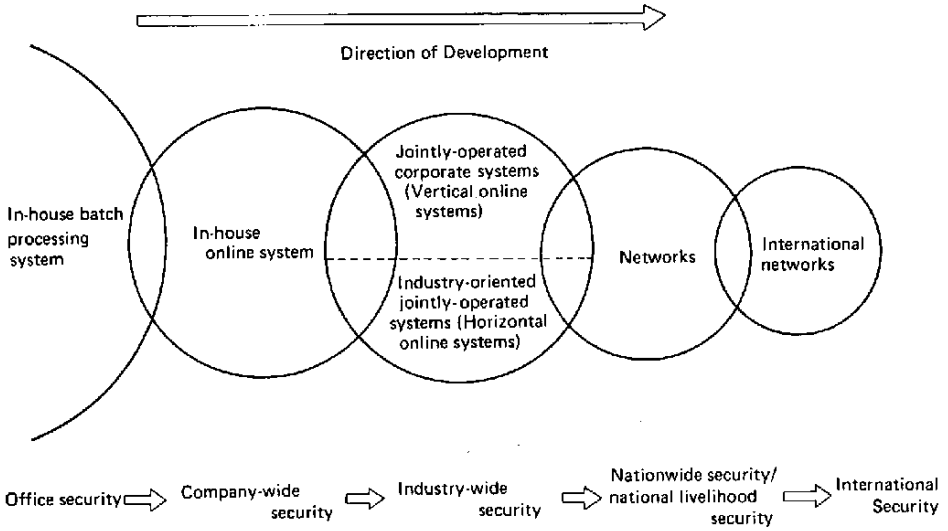


**Figure 1. Computer System Development**

and medium-sized firms and/or into the home. This development has given rise to a variety of new services, to include teleshopping, telebanking and home reservations. The final stage in this evolutionary process involves interconnecting these network systems with international telecom lines to provide domestically-spawned services to users overseas and/or to import foreign-produced services into Japan.

This kind of growth and expansion of computer systems increases and complicates problems related to systems security. What was once simply a matter of in-house security, suddenly becomes intra-group or inter-company security. And the security problems themselves are no longer limited to computers and telecom systems alone, but now entail economic and social security, and in the end, the welfare of the entire nation.

A number of online systems currently operating in Japan are performing work and/or providing services that are vital to the economic and social welfare of the country and the national lifestyle. These systems include the Nationwide Banking System; the Nationwide Cash Dispensing System; the Motor Vehicle Registration and Inspection System of the Ministry of Transport; the Automated Meteorological Data Acquisition System; the Agricultural Information Distributing System; the Social Insurance Online System; and the Emergency Medical Information System. All of these systems constitute nationwide networks, and serve as parts of the nation's central communications "nervous" system. Ensuring the security of these systems is therefore extremely important.

## Realtime Processing

The special feature of online systems is that they are capable of immediately processing data as it is generated. With batch systems, a week's or a month's worth of vouchers are saved up, put together and mailed to the operator of the system. These vouchers are checked upon receipt and passed along to the company's input specialist, who codes the information contained on the vouchers and enters that data into the system. Therefore, all important vouchers related to the handling of goods and/or money are handled like cash, and their careful transfer and storage enable the prevention of errors. When it comes to online systems, however, terminals are installed in the sales and investment departments, and employees input data into them as they talk with customers, which means that there is no opportunity for managers to check the contents of that information. The more terminals are hooked up to an online system, the greater the risk of illegal access by unauthorized persons and/or the illegal entry of false data.

Online realtime processing means that all information requiring processing can be handled on the spot. In the case of banking systems, for instance, this means that account holders can go to any one of their bank's branch offices anywhere in Japan and have funds withdrawn from their accounts and remitted to parties they specify. Online realtime reservation systems make it possible to go to any travel agent and make plane and/or bullet train reservations, and purchase the necessary tickets on the spot. However, these kinds of capabilities also mean that no processing whatsoever can be done when a malfunction occurs anywhere in the system. The more accustomed we become to the convenience of online realtime processing, the greater the confusion that results from a sudden work stoppage. Realtime processing capabilities have increased the importance of systems security.

## Man to Machine

The terminals for batch systems are generally stuck away in a corner of the administrative department, and are operated by input specialists called key punchers. In the case of online systems, terminals are installed out in the open in a number of different departments and are operated by numerous different persons. The ideal situation for operating an online system is to have everyone in the section or department trained to be able to input data into the system via a terminal, even as he or she is talking with a customer. This is because the efficiency of the system will not improve if you have to rely on specific individuals to operate the terminals. However, whereas it is only necessary to supervise the key punchers of batch systems, when it comes to online systems, all the employees that work in every section or department where terminals are installed nationwide require supervision. Training all employees at every sales office, plant or warehouse to operate online system terminals increases the risk of a bad

apple in the bunch using his/her acquired skills to commit a crime. This creates problems from the standpoint of systems security.

This has become especially true in recent years when the proliferation of distributed processing systems and workstations has made it possible for employees from a wide variety of offices outside of EDP departments to operate online system terminals. While this situation has most definitely increased work efficiency and productivity, it has also increased the scope of security coverage required, thus making it harder to implement and enforce security measures.

Generally speaking, it is difficult for an outsider to break into a company and commit a crime using an online system. Conversely, it is very difficult to prevent someone inside the company who has been trained and is familiar with the operation of the online system from committing a computer crime if he/she so desires. Over 60% of all computer crimes committed in Japan using online systems were inside jobs, i.e. were crimes committed by people (employees) inside the company. This points up the extreme weakness of online systems against attacks from within. Technical measures alone will therefore not be enough to achieve and maintain good systems security in line with the spread of office automation and online systems in future. More important than technology-related security measures will be effective personnel management systems and the establishment of a system of work ethics.

## Software Programs: Getting Larger And More Complex

Online systems enable the mutual interconnection of systems run by different firms, and the construction of jointly-operated computer networks that can extend nationwide or around the world. When online systems are interconnected with telephone, telegraph or public facsimile networks it increases the opportunities for large numbers of unspecified terminals to access computer centers. Thus, when designing and building online systems nowadays, we no longer have to deal with the problems this gives rise to inside a solitary company, but rather with the complex relations these create with outside firms, such as customers and subcontractors.

The software used in online systems is actually compilations of numerous simple programs linked together. This makes the logic and construction of this software hard to understand, and its design concepts difficult to comprehend. In fact, online systems software can get so complicated that only the senior systems engineers who designed and built the system are capable of understanding it. Take banking systems, for instance. The various banking operations carried out via these systems, such as savings, loan and exchange operations, are not performed individually, but rather are linked together and processed in succession. In the case of city banks, these programs can reach several million steps in length. If a bug in the software causes a system to malfunction and have

to be shut down, it has become almost impossible to quickly locate the bug responsible for the problem. And systems audits, which play such an important role in systems security, are supposed to be performed by small numbers of auditors, but, in actuality, the task of auditing complicated online systems has become more than a few auditors can handle. Computer education and training is unable to keep pace with the rapid growth and spread of online systems, and the cultivation of systems auditors capable of comprehending entire systems is lagging behind. This has resulted in online systems being operated without systems audits.

Online systems software incorporates huge amounts of corporate knowhow and valuable data, and can be considered a part of a company's assets. If this software is destroyed, stolen and/or resold, the loss to the company involved is great. Online systems software is protected after a fashion by copyright laws and corporate privacy acts, but the current legal system is still unequipped to handle software-related crimes adequately. In future, we will have to establish rules concerning online systems software from an international perspective.

## Centralization And Mass Storage Of Files

All files related to huge nationwide or international online systems comprising tens of thousands of terminals are generally centralized and stored enmasse at computer centers. Remarkable advances in storage media technology have resulted in magnetic disk packs and mass storage memories which have permitted the information centralized at computer centers to grow more voluminous with each passing year. A recent trend evident in online banking systems is to compile individual customer data and other files stored en masse at computer centers to form linked ledger files. This scheme means that even a little bug in a program that controls computer center equipment, telecom lines or terminals can paralyze all the functions of a system, bringing work to a complete stop.

Huge online systems are not merely computerizing the work performed by individual companies or government offices; they are steadily becoming a part of the social infrastructure, supporting key economic and social activities of the entire nation.

One facet of online systems that has become a particularly sticky problem here in Japan is the concentration of online processing centers and databases in the major metropolitan area of Tokyo. Right now more than 60% of all online processing centers and over 90% of all online databases are found in the greater Tokyo area. Consequently, roughly 70% of all software houses in Japan are also located in Tokyo. It goes without saying that this kind of concentration of online processing capabilities and related technologies could prove very dangerous. A big earthquake in the Tokyo area, for example, could effectively paralyze Japan's national data processing and data com-

munications capabilities.

Online system security is no longer a matter of simply protecting corporate profits; it is now directly related to protecting the economic and social functions of the nation, and the livelihood of the nation's citizens. When teleshopping, telebanking, home reservation, home security and other such advanced systems currently being designed and constructed come into widespread use, the role of online system security will expand to include the protection of citizen's livelihood, security and property as well as their individual privacy.

## ONLINE SYSTEM SECURITY MEASURES

As indicated in Figure 2, online systems can be illegally accessed and utilized from a large number of different locations and equipment. These vulnerable locations/equipment can be categorized as follows:

1) Computer Center Equipment (building, computer room, computers and related equipment and building wiring);
2) Telecommunications Lines (Inner city telecom lines, inter-city transmission channels, international transmission channels and relay stations.);
3) Switching Equipment (Switching equipment at telephone offices and private branch exchanges.); and
4) Terminal Equipment (I/O devices and wiring inside users' buildings.).

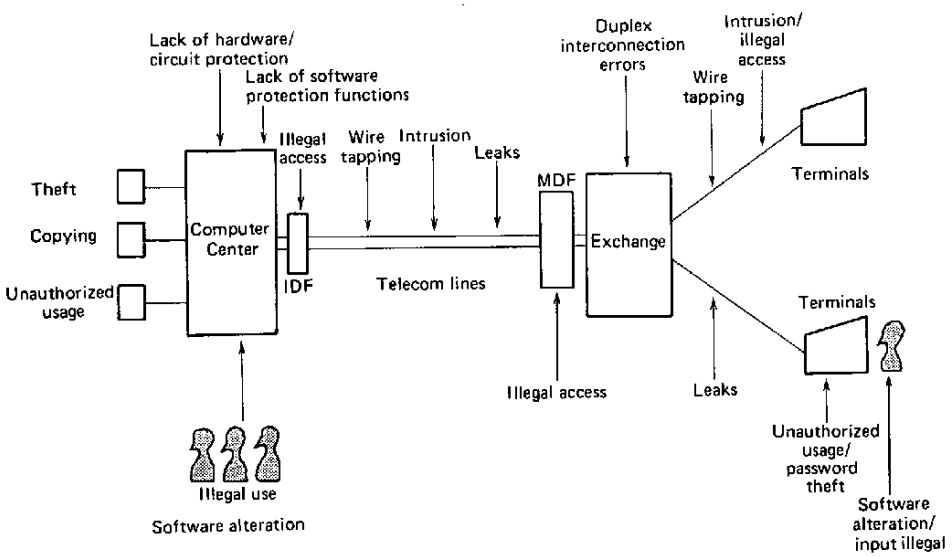


**Figure 2. Principal Threats To Online Systems**

With batch systems it is only necessary to secure the computer center and the equipment installed therein, but with online systems, the number of locations and types of equipment that must be protected are scattered all over the place. Moreover, when there is a system breakdown, the responsibility for ensuring security is for the most part no longer limited to individual companies, but rather is more likely to be distributed among a number of different firms. For example, the user is generally responsible for providing security for the computer center building, the computer room and the hardware installed therein. However, when it comes to dealing with bugs in the operating system (OS) or communications control programs, this is the responsibility of the hardware manufacturers and/or software firms that provided this software. Responsibility for telecom line breakdowns generally rests with the telecom firms that provide these lines to users, but the users themselves and/or the firms that own the buildings in which the users' computer centers are housed must take responsibility for ensuring the security of the wiring in those buildings. When it comes to switching equipment and terminal devices, the responsibility for ensuring the security of these most often falls on the shoulders of the manufacturers and software firms that provided the hardware and programs.

Thus, the online system user is responsible for implementing security measures related to the processing element of the system, while the telecom firm providing the communications lines has to assume responsibility for implementing security measures designed to protect the telecommunications element of the system. Hardware manufacturers must take responsibility for ensuring the security of the equipment they provide to online systems users, while software houses have to assume responsibility for debugging the software programs they created for use with an online system. If each party's responsibilities are not defined ahead of time, then each will be blaming the other when a breakdown actually occurs.

In reality, however, in most cases where a major breakdown occurs it is difficult to determine right away just where the cause for that breakdown exists, i.e. in the computer center's equipment, in the telecom lines or in the terminal devices. In fact, it is often hard to tell immediately if it is a hardware or a software problem. Therefore, if the security measures for online systems are not united and systematized like the systems they are designed to protect, then they will not be effective.

There are three intimately related points that are vitally important to any discussion of online system security measures: economy, efficiency and security. The more security measures you devise for an online system, the higher the costs of that system become. The daily operation of that system also becomes less efficient as a result. For instance, if you utilize a duplex system to avoid downtime, CPU costs automatically double and the system's control programs become more complicated. Or, if you opt for an eight-digit password

over a four-digit one to prevent illegal break-ins by hackers, security will improve, but input efficiency will drop.

The main reasons companies install online systems are to increase productivity and reduce labor. Online systems designers, therefore, are tasked with creating the most economic, yet efficient systems they can. In highly competitive industries, this can result in security measures being giving secondary consideration. Another factor which often contributes toward the omission of security measures in preference of a more economic and efficient system is management's trust in its employees.

The security, economy and efficiency of online systems are intimately related to one another, and should therefore be in balance with one another. If you worry too much about the reliability of your employees or the threat of hackers breaking into your system, and compensate for these by putting too much emphasis on hardware and security measures, you are going to wind up with a system that is very uneconomic and inefficient, and thus does not contribute to your company's competitiveness.

Conversely, when there is little fear of hackers and employees are very loyal and can be trusted completely, hardware and software security measures can be held to the minimum and a truly economic and efficient online system that strengthens the firm's competitiveness in the market can be constructed. However, should a crime ever be committed using this system, the company runs the risk of losing its position of trust in the business community and of having its system destroyed at one fell swoop. What managers should be asking themselves then is just how much security does the firm's online system need.

## TECHNICAL SECURITY MEASURES

The technical security measures covered in this section are being applied to online systems today. However, just which of these is emphasized and/or strengthened differs with the industry involved and the type and nature of system being employed.

### Access Control Function

To prevent unauthorized persons from illegally accessing online systems via terminals, identification codes are provided to operators in advance and these codes are registered in the system in an access log. Each time a person wants to use the system, he/she must input his/her ID code into the system so it can be checked against the access log. Only after this check is made and the input code has been verified can the individual access the system. By keeping a record of all accesses (access history), illegal utilization of the system can be detected quickly.

### Message Checking Function

To prevent illegal entry of data into an online system, three separate security measures are employed. First, a secret

number must be verified by the computer center. Second, since it is possible that these secret numbers might be stolen if they are used for a long time, they are completely changed periodically. Thirdly, for data inputs involving sums of money over a certain set limit, managers must first press a special key to allow that data to be input.

### Encryption Function

To prevent the illegal acquisition of information while it is being transmitted over telecom lines used to interconnect multi-company network systems, encryption methods are employed to ensure that raw data is not being sent out over these lines.

### Automatic Operation Functions

To prevent the theft of computer resources and other malicious acts perpetrated against online systems in the computer and/or terminal rooms of the computer center, it is important to make use of advanced automatic (unmanned) operation techniques and remote diagnostic functions.

### Systems Auditing Functions

Systems auditing functions must be strengthened to prevent or at least more quickly detect criminal acts such as the illegal acquisition or falsification of information stored in online systems by employees authorized to operate those systems.

### System Duplexing

In order to avoid system damage due to earthquakes, floods and/or fires, computer center equipment should be duplexed and distributed to different locations/cities. And to avoid telecom line breakdowns in nationwide network systems, it is necessary to duplex the inner city lines connected to the center, and to use multiple communication routes for inter-city lines.

## PHYSICAL SECURITY MEASURES

### Physical Access Control To Computer Rooms

Physical access to the building housing the computer center, as well as to the computer, magnetic tapes storage and terminal operation rooms located within that building must be strictly controlled using ID cards and other access control methods/techniques.

### Control Of Terminal Equipment

Numerous cases of illegal access, illegal input of data and illegal acquisition of information are the result of unauthorized persons using terminal equipment. For this reason, access to I/O terminals and measuring devices must be strictly controlled. Also, terminal equipment that has been disconnected from the system and is not in use should be destroyed and disposed of completely to avoid the risk of its being put to

malicious use.

### Control Of Intermediate Distribution Frames

It is quite common for the terminals of the intermediate distribution frames (IDF) used to connect computer center building wiring to inner city cables to be exposed and unprotected. If these terminals are used to link up with the telecom lines during online operation, it is possible to monitor the data being transmitted over those lines. The unprotected IDFs found in the basements and on each floor of buildings owned by private companies should be equipped with covers that can be secured with locks. In the case of nationwide networked systems, there are telephone offices, relay stations, IDF and other telecom nodes located throughout the country that could be used to illegally access and utilize the online systems linked together via that network. This makes it necessary for the users of the system and the telecom firms providing the communications lines for it to cooperate with one another in carrying out daily security measures designed to stop persons from monitoring online transmission.

## PERSONNEL CONTROL MEASURES

### Software Audits

A system of software inspections must be established whereby persons not affiliated with the development of the software used in the online system audit that software to check its data processing integrity.

### Personnel Control Measures

People from various occupations and companies work in the computer and terminal rooms of online centers, to include the user company's employees, technicians and engineers from the manufacturer of the computer hardware used in that system, software engineers dispatched from their companies, telecommunications engineers and workers from subcontractors affiliated with the user firm. It is therefore necessary to put someone in charge of ensuring these people wear ID cards with their photographs attached, of clarifying what every person is doing in the center and of monitoring their work.

### Utilization Of Test Data

When programs are debugged, never use the original files, but rather use test files and test data. This is because when the original file is used, it is possible to record bank account numbers and secret numbers, data which could very well be used to commit a computer crime at some later date.

### Emergency Measures

If a nationwide online system breaks down, work will stop and confusion will reign at all locations interconnected via

that system throughout the country. People should therefore be selected and organized to implement emergency measures designed to deal with such breakdowns. These measures should include methods for switching over to processing of work by hand; procedures for restoring the system; and means of informing customers of the situation. Mock breakdowns should be scheduled at least once a year to enable the computer center and all sites interconnected thereto to practice the emergency measures just discussed.

### Human Relations Management

The formulation and implementation of security measures will strengthen an online system against attacks and breakins from outside, but are all but useless against attacks from within. That is, if an employee of a user of an online system decides he/she wants to commit a crime using that system, all the technical security measures in the world are not going to be able to prevent him or her from doing so. Human relations management holds the key to preventing "inside jobs" such as this. It is thus very important that human relations management be strengthened through in-house education and training; regular meetings; and the establishment of career-oriented programs.

## FUTURE PROBLEMS

The future spread of online systems and their utilization will raise some major problems from the standpoint of systems security. For example, as the propagation of online systems continues, terminal equipment is going to find its way onto the desks of small- and medium-sized business employees as well as into the home. This is going to increase the importance of security. As online financial, distribution and transportation systems penetrate into every aspect of the nation's economic and social activities, daily living will be made much easier and more convenient. The more accustomed to the convenience afforded by online systems that the nation's citizens become, the bigger the impact systems breakdowns will have.

Another problem has to do with the pace of technological development. Security measures tend to lag behind advances in computer technology. The technologies employed to achieve systems security will continue to compete with those used to commit computer crimes. If security-related technologies lose out to crime-related technologies, then online systems will cease to exist.

As pointed out above, the strengthening of technical security measures can, to a certain extent, prevent system malfunctions and computer crime. However, technology alone is not enough. Human-oriented security measures are also very important. Measures designed to raise morale at the workplace and the establishment of work ethics for employees engaged in information processing tasks are vital. If this kind of human relations management is neglected, then even huge investments in security mea-

sures will not prove effective.

Market competition is fierce, and users of online systems expect their systems to be economical and efficient. Designers of online systems, therefore, have a strong tendency to slack off on the security-related aspects of new systems in favor of providing the user with greater economy and efficiency. However, should there ever be a major breakdown or crime involving this type of system, then the user company(ies) would suddenly be viewed as untrustworthy and unreliable, and would lose customers as a result. Managers must devote sufficient time and effort to studying the proper balance of economy, efficiency and security for the online systems they use.

Certain industries using computer networks are switching from traditional paper-based transactions to electronic transactions. However, in order to protect the consumer in this type of environment, it is important to lay down rules concerning electronic transactions, rules that define at what point an electronic contract becomes valid, at what point such a contract can be nullified, and/or the procedures for dealing with damaged and/or defective goods.

Rules governing the amount and type of compensation required when breakdowns in electronic accounts settlement systems result in losses are also needed. This is because when something goes wrong with an online system used in the settlement of accounts, there is no way of proving whether or not the users of that system were responsible for the breakdown and resulting losses. Since it is practically impossible to try and ensure the security of online systems via technical security measures alone, compensation and insurance schemes will have to be established and backed up with appropriate legislative measures.

Countries like the United States and West Germany are revising their legal codes to deal with increases in computer crime. However, there are still large numbers of nations where the criminal penalties for stealing data, destroying software and/or engaging in hacking activities are lacking. There are even countries that do not have legal sanctions for dealing with violations of privacy and/or copyright infringements. Computer technology is advancing and spreading at a rapid pace, but social and humanitarian studies aimed at supporting these systems are way behind. In future, we will have to promote academic and industrial research into these areas at the international level.

# COMPUTER CRIME AND THE LEGAL SYSTEM

Yoji Yamashita
Adviser
Research Department
JIPDEC

## CURRENT STATE OF COMPUTER CRIME

There are a number of different thoughts concerning what constitutes a computer crime, but for our purposes here we shall define computer crime as illegal acts perpetrated against computer systems, and/or the use of computer systems for illegal purposes.

### CD Crimes

Computer crimes adhering to this definition can be broadly divided into two types: CD crimes and all others. CD crimes are crimes involving the misuse of cash dispensers (CDs), those computer system-based automatic cash dispensing machines utilized by banks and other financial institutions. Table 1 shows the number of CD crimes and related arrests in Japan between the years 1975 and 1986 according to records kept by the Japanese National Police Agency (NPA).

As you can see, CD crimes have increased remarkably in recent years. A primary factor contributing to this phenomenon has been the sudden increase in CDs (this includes automatic teller machines (ATMs) as well) and the plastic cash cards used to operate them. For example, as of 1986 there were 56,000 CDs in operation in Japan, and the number of cash cards that had been issued by that year exceeded 130 million. This worked out to 4.8 times as many CDs and 3.5 times as many cash cards as there were in 1978.

The most common CD crime is to steal

**Table 1. Number of CD Crimes and Related Arrests Between 1975 and 1986**

| Year | No. of CD Crimes | No. of Related Arrests | Year | No. of CD Crimes | No. of Related Arrests |
|---|---|---|---|---|---|
| 1975 | 8 | 5 | 1981 | 288 | 179 |
| 1976 | 23 | 18 | 1982 | 472 | 321 |
| 1977 | 64 | 40 | 1983 | 642 | 503 |
| 1978 | 131 | 72 | 1984 | 723 | 575 |
| 1979 | 187 | 94 | 1985 | 929 | 828 |
| 1980 | 212 | 99 | 1986 | 886 | 716 |

someone's cash card, figure out the secret number and then use that card to withdraw money from the victim's bank account. This modus operandi accounted for 74% of all computer crimes perpetrated during 1984, and for 90% of all the computer crimes committed during 1985. There were also numerous cases where someone found a lost cash card and used it to illegally withdraw money from the card owner's bank account.

A number of different methods are used to learn a cardholder's secret number. In many cases, the criminal is acquainted with the cardholder and knows the secret number before he or she steals the card. In 47% of all CD crimes perpetrated in 1985 using stolen cash cards, the criminal was already aware of the cardholder's secret number. Other methods used to figure out these secret numbers include finding out the cardholder's date of birth and/or telephone number and then experimenting with these numbers until the secret number is discovered. There are also numerous cases where the cardholder writes his/her secret number on the card itself so as not to forget it. Although a less frequently used ploy, cash card thieves have been known to steal a person's cash card and then trick the unwary cardholder into revealing his/her secret number. There have also been cases where employees of banking and other financial institutions have found lost cash cards and then used their company's card readers to "read" the secret numbers.

The types of CD crimes just described are rather simple in nature. However, during the past several years we have witnessed much more complicated CD crimes involving computer specialists who have actually forged cash cards.

One example of such a crime was perpetrated in 1981 by a former bank employee. Prior to his retirement, this person had been in charge of that section of the bank's online center responsible for making up cash cards. After he retired, the man returned to the online center on a holiday and used the center's magnetic tape readers to obtain depositor's secret numbers stored on a data file. He then input these secret numbers onto blank cash cards, and used the resulting forged cards to withdraw money from unfortunate depositors' bank accounts via CDs.

Another example of a high-tech CD crime took place in 1985. The culprit in this case was a computer software firm engineer who had been dispatched to the online center of a certain bank. This person took advantage of his special access to the equipment installed inside the center to forge bank books. First, he selected only large depositors who made few deposits and/or withdrawals. Then he extracted the secret numbers encrypted in their bank account numbers, decrypted these and forged bank books by inputting this data onto the blank magnetic strips of unused bank books. Finally, he took these forged bank books and used them at the bank's ATMs to withdraw money from the unwary depositors' accounts.

Card readers have been sold on the

open market for the past few years now, meaning that anybody who can afford to buy one can use it to read the secret numbers on cash cards. In an attempt to prevent crimes arising as a result of this capability, banks have taken to either encrypting these secret numbers, or doing away with the system of inputting secret numbers onto the cards altogether in favor of recording these numbers at the center itself for checking there. In the case of the latter, depositors' secret numbers are encrypted prior to being recorded. Nevertheless, even this kind of security system isn't very effective against computer specialists with access to an online center's key equipment if they decide they want to utilize that equipment for their own illegal gain.

A third example of a high-tech crime involving CDs was carried out in 1980 by a technician who worked for a public corporation that owns and upkeeps its own telecommunications lines. This CD thief used specialized equipment to "tap" the telecommunications lines used to transmit cardholders' bank account numbers and secret numbers to computers at banks' online centers each time a CD was operated. After acquiring, recording and digitalizing this data, he was able to collate it with the information contained on the magnetic tape attached to his own cash card. In this manner he "read" the secret data contained on cards held by 21 bank depositors. He then forged new cash cards by recording the bank account and secret numbers he had obtained onto test cards kept at his company. The thief was then able to use these forgeries to withdraw money from depositors' bank accounts via CDs.

All of the CD crimes cited above were perpetrated by individuals acting alone. Unlike the United States, Japan has not yet had to deal with a CD crime carried out by syndicated crime.

There have also been a number of cases where CD networks have been used for illegal purposes. For example, there have been incidents where kidnappers demanding ransom money and/or extortionists threatening companies have had their victims electronically transfer money to specified bank accounts and then withdrew those monies from the accounts via CDs.

## Other Computer Crimes

Figures concerning computer crimes in Japan other than those involving CDs are presented in Table 2.

As you can see, whereas there were only 14 computer crimes committed during the ten year period between 1971 and 1980, a total of 61 such crimes were carried out during the next six (6) years between 1981 and 1986. In other words, computer crime has increased rapidly in line with the recent widespread use of computers.

Table 3 categorizes the computer crimes committed in Japan between 1971 and 1986 as to type of system (business) and whether they were inside or outside jobs.

The figures presented in Table 3 were gleaned from NPA records. Other sources of information regarding computer crimes

**Table 2. Numbers and Types of Computer Crimes Other Than CD Crimes Between 1971 and 1986.**

| Type of Crime / Year | Unauthorized Data Input | Unauthorized Acquisition of Computer Programs and Data | Destruction of Computer Hardware | Unauthorized Utilization of Computers | Alteration/ deletion of Computer Programs | Total |
|---|---|---|---|---|---|---|
| 1971 | | 1 (1) | | | | 1 (1) |
| 1972 | | | | | | |
| 1973 | 1 | | | | | 1 |
| 1974 | 1 | | | | | 1 |
| 1975 | 2 | | 1 | | | 3 |
| 1976 | 1 | | | | | 1 |
| 1977 | | | | | | |
| 1978 | 3 (1) | 1 | | | | 4 (1) |
| 1979 | 3 | | | | | 3 |
| 1980 | | | | | | |
| 1981 | 6 | 1 | | 3 (1) | | 10 (1) |
| 1982 | 5 (1) | 1 | | | | 6 (1) |
| 1983 | 4 | 2 (1) | | | | 6 (1) |
| 1984 | 8 | 2 | | 1 | 1 (1) | 12 (1) |
| 1985 | 9 (2) | 1 | | | | 10 (2) |
| 1986 | 13 | 1 | 2 | 1 | | 17 |
| Total | 56 (4) | 10 (2) | 3 | 5 (1) | 1 (1) | 75 (8) |

Note: Figures in parentheses indicate offenses which were not acknowledged by the police, but which were reported in newspapers and other publications.

other than CD crimes indicate that 83% of such crimes committed in Japan between 1971 and 1980 were perpetrated by individual persons working alone, while only 13% were attributed to two or more people working together. However, this same information indicates that during the five year period 1981 through 1985, the ratio of non-CD computer crimes committed by individuals working alone dropped down to 60% of the total, while group perpetrated crimes rose to 36% of all such crimes committed during that period. Furthermore, of those computer crimes committed by two or more people working as a group, 40% were carried out as a result of collusion between people inside the organizations targetted and outside partners.

## False data input

Computer crimes involving the input of false data into a computer system are the most numerous in Japan. A very common scenario in this type of crime is where a bank clerk uses a computer terminal to deposit nonexistent funds into a false bank account he has created in advance for just that purpose. Another often seen scenario is the one where a branch manager or clerk of a banking

**Table 3. Computer Crimes Committed Between 1971 and 1986 by Type of System (Business) and Whether or Not They Were Inside Jobs.**

| Type of System (Business) \ Type of Crime | Inside Job (Note 1) | Outside Job | Unknown | Total |
|---|---|---|---|---|
| Commercial Bank | 10 | 2 | 1 | 13 |
| Agricultural Cooperative | 18 | | | 18 |
| Trust Bank (Note 2) | 3 | | | 3 |
| Post Office | 1 | 2 | | 3 |
| Consumer Finance Association/ Credit Union | 6 | | | 6 |
| University | | 1 | 2 | 3 |
| Public Agency | 9 | | | 9 |
| Other | 15 | 4 | 1 | 20 |
| Total | 62 | 9 | 4 | 75 |

Note 1: Even in cases of collusion, if one member worked for the organization that was victimized, it is considered an inside job.

Note 2: Trust Banks are defined here as small-scale local financial institutions that serve both consumers and corporations.

institution prepares a false voucher for a loan, and then inputs that information into the bank's computer system via a terminal, electronically transferring the amount indicated on the voucher to a false bank account. There have also been cases where individuals have entered false information onto vouchers and other such bank forms and then had clerks unwittingly input this data into the bank's computers.

Practically all of these types of crimes are inside jobs. And the reason employees can pull off such crimes is because of organizational and/or managerial weaknesses within the banks themselves. Either the employees who commit such crimes are given total responsibility for the carrying out of their assigned tasks (i.e. are not supervised properly), or else executives in charge have complete authority over their sections/offices, and are not directly responsible to anyone for their activities.

There are also examples of computer crimes committed by groups of people as opposed to individuals. With these kinds of crimes, certain members of the group generally work inside the target organization while the rest are outsiders, i.e. people not directly affiliated with the organizations they rob. One example of such a computer crime in Japan was perpetrated around 1983/84 by a policeman. The policeman in question forged a driver's license registration ledger, then convinced the operator of the computerized police driver's license system to input the data contained in that ledger into the system. The policeman managed to make 43 false driver's licenses, which he then sold through an outside inter-

mediary.

In 1986, an outside group made use of one of its member's knowledge of computers and computer systems to alter 150 losing horse betting tickets so that an automatic payoff machine would accept them as winning tickets. The group duped the payoff machine out of 80 million yen. This incident brought to light a bug in the automatic payoff system at the horse track in question.

There was a computer crime related to the inputting of false data that took place back in 1981 and involved all the executives of a particular company. The company in question specialized in carrying out construction work on railroads. After their construction materials were damaged by a flood, the company decided to inflate its losses in order to receive additional compensation. It did this by embellishing the figures logged in its computerized accounting system to reflect higher purchase costs.

## Unauthorized acquisition of data and computer programs

### Unauthorized acquisition of data

There have been two computer crimes involving the unauthorized acquisition of data in Japan that can be cited as typical examples of such incidents. The first occurred back in 1970 when someone copied and sold a certain monthly magazine's list of subscribers recorded on a magnetic tape. This tape was copied while on loan to the company in charge of mailing out the monthly magazine to subscribers.

The other typical example of unauthorized acquisition of data took place in 1983 when a section chief at a public corporation responsible for maintaining data on compact car owners, new car registrations and inspection periods smuggled a magnetic tape containing this data out of the company long enough for his partner in crime to make copies of it. The two then sold these copies.

Another more recent example of this type of computer crime made the newspapers in 1987. According the articles written about this incident, the information manager at a department store copied a magnetic tape containing that department store's customer list. He then passed this information through a broker friend of his to a company that specializes in making up and selling mailing lists. The ever increasing need for good customers to ensure corporate sales growth is expected to contribute to a rise in this type of crime in future.

### Unauthorized acquisition of computer programs

The following are two well-known examples of computer crimes in Japan involving the unauthorized acquisition of computer programs. The first took place in 1982 and was perpetrated by an acting department head of a major Japanese machine manufacturing company. This individual was a key member of the company's computer-aided design (CAD) system development team. Dissatisfied with the company's policy to discontinue sale

of its CAD systems to outside firms, he decided to leave the company and sell CAD systems on his own. In order to achieve his goal, he and an accomplice smuggled a magnetic tape and blueprints containing information related to the company's CAD system out of the company and made copies of them prior to returning them.

The second example of unauthorized program acquisition occurred in 1984. The manager of a newspaper circulation company teamed up with an executive of a software house and one of his programming instructors. The newspaper circulation company manager furnished the software house employees with a floppy disk containing a program developed by the circulation company for processing information on newspaper delivery procedures, monthly bill collecting and sales expansion methods. The software people input this program into a microcomputer, saved it to memory and produced a pirated copy of the original program. The software house then leased this program to newspaper circulation firms nationwide.

### Hackers

The first major hacking incident in Japan was initiated back in late 1984 and continued through early 1985. While a branch office of an American firm was using Kokusai Denshin Denwa (KDD) Co., Ltd.'s VENUS-P international data transmission service system to exchange inventory data with its home office in the United States, a hacker electronically lifted that firm's password during transmission. Following this, the hacker made illegal use of KDD's VENUS-P telecom lines to break into the databases of more than a dozen U.S. companies and steal hobby-related information.

There were other hacking incidents in Japan in 1985 as well. Among them was a series of crimes involving hackers from four (4) different European countries who broke into the computer systems of a Tokyo database firm and a university research institute, both of which subscribed to KDD's VENUS-P services. These European hackers stole certain data and altered other, the latter being equivalent to a sort of electronic graffiti. Also in 1985, 20 hackers from West Germany somehow obtained the password for the computer system installed at the Japanese government's High Energy Physics Laboratory and used it to illegally access that system.

## Destruction of computer hardware

Two good examples of computer crimes involving the destruction of computers and/or computer-related hardware in Japan were perpetrated by members of Japanese ultraleftist radical groups in 1975 and 1978. The 1975 incident involved the bombing of the computer room of a major Japanese construction firm. In 1978, radicals opposed to the Narita International Airport severed the data communication cables used in that airport's computer-controlled management system.

More recently, a group of local toughs

broke into a pachinko (Japanese-style pinball) parlor in 1986 and destroyed the computer system used to control the operation of the pachinko machines. This willful act of computer destruction was reportedly done to get back at the owner of the pachinko parlor for not purchasing tickets to a dinner show that the toughs tried to push off on him.

### Unauthorized utilization of computers

In 1981, 106 employees of a Japanese public corporation made unauthorized use of their firm's computer system to tally up bets placed and monies won in an in-house baseball pool. Another incident of unauthorized computer utilization also took place in 1981. In this case, an employee of a personal computer shop used a password written on a memorandum left behind in the shop by a customer affiliated with a certain Japanese university to access that university's computer system. The shop employee utilized his access time to demonstrate certain computer operations for customers visiting the personal computer shop.

### Alteration/deletion of computer programs

There was a very serious incident of computer programs being deleted from a computer system in Japan in 1984. It is still not known who committed this crime, but whoever it was erased 2,500 academic/scientific programs from magnetic disks used in a computer system installed at a certain Japanese university research institute.

## PITFALLS FACING COMPUTER SECURITY LEGISLATION

Some are of the opinion that there is a need to enact legislation aimed at standardizing security measures against computer crime and making owners of computer systems responsible for applying these measures to their operations. Some of the arguments put forth in support of this opinion are:

—Computer networking is becoming more widespread, and the more it advances the greater the need for uniform security. Weak security measures at any one link in a network system jeopardize the entire network by leaving it open to the risk of computer crime. For example, last year blank cash cards and a data writer (device used to enter pertinent data onto the magnetic tape portions of cash cards) were stolen from a branch office of a certain banking house and used to forge false cash cards. This is indicative of the type of risks involved when security measures are not enforced uniformly by all members of a network system;

—Computer system owners are not the only ones who are victimized by computer crimes. The users of these systems are also often the victims of computer crimes. This holds especially true when it comes to bank depositors who use the CD and ATM systems to do their banking;

—Even if legislation aimed at punishing perpetrators of computer crimes is enacted, if records of the data sent and received via online system terminals are not properly maintained, then it will be impossible to uncover and gather the evidence necessary to prosecute these criminals;

—According to the results of a 1985 NPA questionnaire aimed at companies from a variety of fields listed on the stock exchange, 80% of the respondents indicated that they felt computer security was insufficient.

The more generally held opinon, however, is that there is not a need for legislation designed to standardize computer security measures. Some of the reasons given in support of this are:

—The level of security required by system owners differs according to the type of business they are in and the kind of environment they are operating, thus making standardization very difficult. Even system operators from the same industry use different types of systems, which means the risk of computer crime differs according to the system. This requires that security measures also differ according to the situation;

—Strict security measures require large sums of money to implement and can hinder processing efficiency. Specific security measures should therefore be promoted on a case-by-case basis, taking into consideration the necessity and effectiveness of such measures vis-a-vis their demerits from a cost-performance standpoint. This is perhaps easier said than done since it will be difficult to avoid a certain degree of uniformity when it comes to legalizing computer security measures;

—Since the cost of security measures is unrelated to the size of the system or company employing it, uniform compulsory laws will place an extremely heavy investment burden on small- and medium-sized firms and could well prove an obstacle to these firms' informatization schemes;

—Even if legislation is enacted that makes it mandatory to implement the minimum security criteria, advances in technology could nullify the significance of these criteria relatively quickly.

For these reasons, the Japanese government is going to set forth certain computer security criteria which computer manufacturers and users will then use as a basis for devising their own security measures.

Nevertheless, as it stands now, security measures designed to prevent computer crime are insufficient at best. To make up for this, attention is being focused on criminal laws as a means of curbing computer crime.

To commit a computer crime, a person must possess a certain degree of knowledge related to computers; however, unlike ordinary criminals, he doesn't require any special physical or mental capabilities. This is because committing a computer crime can be as simple as pushing a few keys on an input terminal when no one is looking. Motivating factors behind computer crimes can range from a need for money to a desire to challenge a system's security measures. Since it is believed

that many computer crimes are perpetrated only after the risk of being caught and punished has been carefully weighed, the intimidation factors inherent in criminal law could prove rather effective.

## AMENDMENTS TO THE PENAL CODE

### Nature Of The Penal Reforms

Computer crime legislation in Japan was first realized this past spring in the form of partial amendments made to the Japanese penal code. These amendments were put into effect as of 22 June 1987.

As stated previously, this legislation will not apply to all acts that are ordinarily categorized as computer crimes. Although the new legislation will cover most crimes related to computers, acts such as the the unauthorized acquisition of data and computer programs, the unauthorized utilization of computers and/or the unauthorized entry into a computer system simply to "see" what is there are not considered crimes punishable by law.

The reason for creating this kind of legislation, i.e. legislation that does not cover all offenses related to computers, was to avoid touching off a major dispute over whether or not acts not traditionally considered criminal behavior should suddenly be made punishable by law. In numerous instances, false data input, the unauthorized deletion of computer data and/or programs, destruction of computer hardware and CD crimes can be prosecuted under existing laws. However, even in these cases, quite a few computer criminals get off on technicalities due to loopholes in pertinent criminal legislation. The recent rapid rise in computer crime made it painfully clear that something would have to be done, and quickly, to close the loopholes in existing criminal laws. The amendments to the penal code earlier this year were carried out for the express purpose of closing those loopholes by expanding the scope of existing laws dealing with document-related crimes, crimes related to the obstruction of business and fraud. This approach to computer security legislation didn't call forth much protest and the bill passed the Diet rather easily.

### Contents Of The Amendments

#### "Electromagnetic records" and "electronic computers"

Amended legal provisions define the concept of "electromagnetic records" as "Records made by electronic, magnetic or other means that cannot be perceived by third parties, and which are used in electronic computers to process data." This definition refers specifically to that data stored on integrated circuit (IC) memory chips, magnetic tape, magnetic disks and optical disks, and applies to computer programs recorded on these media as well. It does not apply to data that is being transmitted or processed.

There are no provisions in the criminal code that define the concept of an "electronic computer." However, typical examples of such machines are given as general-purpose computers, small business

computers, personal computers and computers used in process control applications. The criminal code also interprets electronic computers as encompassing those microcomputers incorporated into other types of machinery.

**Illegal creation, use and destruction of electromagnetic records**

In the past, the altering of electromagnetic records as a result of the inputting of false data was not treated as a document-related crime. This was because there was a substantial difference between a "document" and an "electromagnetic record" as far as legislation regarding document-related crimes was concerned. That is, a document is something that can be seen and read. And even in the case of documents, only those produced by specific persons, and/or which express corporate thinking and ideas come under the purview of document-related crimes. By comparison, electromagnetic records are not visible to the naked eye, and newly input data can be processed together with other data using computer programs to create yet different data. More often than not, this process involves the thinking and actions of numerous different people, and thus makes it very diffficult to view electromagnetic records in the same light as documents produced by specific individuals.

Nevertheless, today electromagnetic records are taking the place of documents, and just like documents, are serving as instruments of proof. Because electromagnetic records are now being used as proof of certain facts, new criminal provisions were enacted to protect these non-documentary records.

For example, it is now a crime to illegally create electromagnetic records for the purpose of falsifying work processed by a third party. It is also a crime to utilize electromagnetic records created in this way to process said work. Destroying (deleting) electromagnetic records related to rights and duties is a crime, too. The term "to illegally create electromagnetic records" as used here can be interpreted as a lack of authority to create such records, or as the improper use of the authority to create electromagnetic records. Only those electromagnetic records related to rights and duties, or which serve as proof of a fact, fall under the purview of the penal code. This makes crimes involving such electromagnetic records similar to the document-related crime of forging private documents.

Persons committing the crime of illegally creating or using illegally created electromagnetic records related to rights, duties or proof of facts are subject to up to five-year's imprisonment and/or can be fined up to 200,000 yen. People who destroy or delete electromagnetic records related to rights and/or duties can be imprisoned for up to five years.

These penalties are more severe for those individuals who illegally create public electromagnetic records (up to 10-year's imprisonment and/or 400,000 yen), or who record false data on electromagnetic records that serve as the basis for public certificates (up to five-year's

imprisonment and/or 200,000 yen).

**Computer destruction and the obstruction of business**

Traditionally speaking, the crime of obstructing business was premised on the fact that a person was in the midst of performing work when he/she was duped or forced to do something not related to that work. However, the obstruction of business using computer systems can involve the deletion of data and/or the inputting of fake programs that destroy computer's operations. These actions are directed against computers, and in no way involve the duping or threatening of human beings. This form of business obstruction was viewed as a new type of crime, and stiffer penalties were levied on people committing these crimes (Whereas crimes related to the obstruction of business used to earn offenders up to three-year's imprisonment and/or 200,000 yen fines, business obstruction involving computers demands up to five-year's imprisonment and/or 400,000 yen in fines.).

Those acts directed against computers and/or computer systems which are considered crimes related to the obstruction of business consist of 1) the destruction of business computers and/or the electromagnetic recording media used therein; 2) the entering of false information and/or illegal commands into a business computer (When we speak of illegal commands here we are refering to altered or modified programs that are run illegally, and to the inputting of illegal commands while a program is being run); and 3) other destructive acts that directly impact the operation of a computer system, such as the destruction of a power source and/or the cutting of telecommunications lines.

The acts of destruction outlined above are crimes because they prevent computers from operating in the ways they were designed to operate, and/or create situations wherein computers operate differently from their intended purposes, thus obstructing the conduct of business.

**Utilization of computers for fraudulent means**

The most common form of computer fraud is to use a computer terminal to enter false funds transfer data into an already existing account. However, the computer system itself is the victim of this kind of fraud; nowhere is the prerequisite for a fraud case, i.e. a person being swindled, evident. Now if the funds fraudulently transferred into the existing account are withdrawn in the form of cash, then a case can be made for larceny. But if those funds are simply left in the account as is, the general interpretation of the law is that it does not constitute larceny. In order to prosecute these kinds of acts, new legislation covering the use of computers for fraudulent means was enacted. The penalty for violating this law is up to ten-year's imprisonment, the same as that for ordinary fraud.

The first type of crime covered under this new law is that of inputting false data and/or illegal commands into a computer system to create a false electromagnetic

record related to the acquisition and/or loss (changes) of property rights. For example, it is now a crime to create a false account balance record in the electronic accounts ledger file of a bank's online system. The second type of crime covered under the new law governing the use of computers for fraudulent means is the use of falsified electromagnetic records related to the acquisition and/or loss (changes) of property rights. An example of this type of crime is when someone uses a prepaid card that has been electronically altered to reflect more usages remaining than actually exist. In other words, it is now a crime to use computers to make a profit illegally or to make a third party profit illegally from that act.

## Future Legal Problems

In the past, Japan did not recognize the unauthorized acquisition of computerized data and/or programs as being a crime, with the exception of those things protected under the copyrights law. The need to establish new legislation aimed at covering these types of acts was therefore questioned. When this issue is taken up in future, it will probably be necessary to consider it from two angles, that of the protection of computer systems and that of the protection of data. From the standpoint of protecting computer systems, security violations will most likely constitute the conditions required for a crime. In that case, the problem will arise as to just how much security is required to adequately protect computer systems.

The next type of legal problem facing us in the future has to do with the contents of information. When it comes to business information, how are we going to objectively judge the value of business data? How are we going to handle the transfer of information from one company to the next as a result of employees changing companies in mid career? How are we to deal with employees who leak "secret" information to outside persons concerning their companies' pollution of the atmosphere, for example? These issues should probably be considered from the standpoint of mutually complimentary civil and criminal responsibility. And what about personal data, should it be dealt with based on the protection of individual privacy, or should it be handled from the standpoint of corporate property?

Lastly, the general opinion seems to be that treating stolen machine time and unauthorized computer system access as crimes is carrying things too far. However, there are certain computer systems which stand to lose a great deal from intrusions such as these. It is therefore going to be necessary to come up with legislation aimed at coping with these kinds of acts from the point of view of protecting the computer systems themselves.

# SYSTEMS AUDITING

Moriyuki Torii
Consultant
Research Department
JIPDEC

## HISTORY OF SYSTEMS AUDITING

### Computerization And Accompanying Problems

The computerization of accounting processes in Japan has made remarkable progress from around the mid-1960's, bringing with it a number of new problems.

First of all, by law, accounting books had to be paper-based, and had to be capable of being read by human eyes. Therefore, the maintenance of magnetic tape accounting records was not recognized. The requirement to maintain accounting records in hard copy form proved a major obstacle to computer users hoping to rationalize their accounting processes. A call went up to revise legislation dealing with the keeping of accounting records.

The computerization of accounting work turned accounting into a "black box" operation which made it impossible for certified public accountants (CPAs) to trace the accounting process during auditing. This was a problem since it hindered CPAs in their auditing of financial statements.

### Handling Of Evidentiary Tax-related Data

Computer utilization was and still is being promoted as a means of achieving more rational and efficient, and thus more economical business processing. But requirements that had to be adhered to for tax purposes were holding computerization back. That is, computer users were of the opinion that accounting work could not be computerized because of the tax requirements then in effect.

In an attempt to find a way around this problem, the Japan Information Processing Development Center (JIPDEC) in April 1966 submitted a paper to the Tax Administration Agency titled "Demands Regarding the Handling of Evidentiary Tax-related Data in Line With Increased Computer Utilization." These demands can be summed up as follows:

1) When the contents of calculation processes and results are presented in the required readable format, the contents of the media containing these processes and results should be recognized as legitimate data for storage and maintenance provided the processes/results were performed/arrived at via legitimate calculation methods;

2) Operating processes and procedures (computer programs and flowcharts) which have been acknowledged and registered by CPAs, auditors and other similarly authorized experts should be treated as legitimate processes and procedures; and
3) The contents of internal and external recording media such as cards, paper tape, magnetic tape, magnetic disks and magnetic drums to which original evidentiary data has been transferred should be recognized as being equivalent to the original data.

In short, then, these three demands were submitted to the tax authorities because we wanted them to recognize the magnetic recording media used in computer processing as legitimate records for the purposes of processing taxes. Although the tax office never officially responded to these demands, it did initiate a system of agreements with individual companies by which it formally recognized these demands on a case-by-case basis.

## Need To Revise The Commercial Code

Problems related to the computerization of accounting work stemmed primarily from the ledger regulations of the commercial code. Provision 32 of the commercial code stipulates that "A merchant must keep accounting books and balance sheets that clearly indicate the assets and profits/losses of his business." Computer users demanded that accounting books as defined in this provision should include accounting records stored on magnetic tape and other forms of computer storage media.

In December 1969, JIPDEC submitted a report to the Minister of Justice and to the Chairman of the Commercial Code Subcommittee of the Legislative Council titled "Demands Related to the Revision of the Commercial Code." The commercial code revision proposals contained therein were aimed at facilitating the widespread use of computers in the accounting and financial departments of companies for the purpose of rationalizing and modernizing corporate accounting and financial processing and contributing to the improvement of business operations. The main points of the commercial code revisions concerned the creation and storage/maintenance of documents and their perusal. In brief, these points were as follows:

1) Accounting books, financial statements and other important documents related to a company's operations, as well as stockholder name lists, debenture registers and other documents that businesses are required to prepare and maintain under the provisions of the commercial code can be created and stored/maintained on punched cards, magnetic storage media (magnetic tapes, disks and drums), microfilm and other data storage media. However, documents stored and maintained using these methods must be capable of being transferred to paper (hard copy form) that can be clearly and easily read for a considerable period of time; and
2) When a merchant stores documents

using the above cited methods, stockholders and other parties with the right to peruse and/or make copies of those documents can request that the merchant transfer that information to paper (hard copy form) that can be read clearly and easily for a considerable period of time.

In response to these demands, the Ministry of Justice proclaimed that microfilm can be interpreted as a readable document under existing legislation. Furthermore, it appended a second section to provision 32 of the commercial code which states that "Interpretations of regulations related to the creation of commercial ledgers must take into consideration fair accounting practices." These decisions have served as a partial solution to the problem of commercial code revisions.

## Systems Auditing Proposals

In the mid-1960's, the focus of attention was limited to the legal and auditing problems related to the computerization of accounting work. But upon entering the 1970's, computer-related crimes began to rise here in Japan, and privacy protection movements were started by people from various walks of life.

Since it became obvious that problems arising from computerization were not limited to accounting work alone, JIPDEC undertook to come up with new measures to deal with these problems. This resulted in the temporary suspension of research on accounting and tax-related problems that had occupied most of its time to date, and the start of new research activities related to systems auditing in an effort to formulate solutions to a wide range of problems affecting information systems.

In 1974, JIPDEC had to start from scratch on its research into the auditing of information systems, labeling its efforts as the study of "systems auditing." The following year, in 1975, JIPDEC established a Systems Auditing Committee and asked Yuichiro Kaneko, then chairman of the Federation of Economic Organizations' (Keidanren) Economic Information Legislation Committee, to chair the new committee. It then set up a Theoretical Subcommittee and Technical Subcommittee under the jurisdiction of the new Systems Auditing Committee and commenced research work. Two reports put together by this committee in the interim, "How To Conduct Systems Auditing In Japan" (published in March 1976) and "The Road To Establishing A Systems Auditing System" (published in March 1977), were widely read in Japan and spurred the spread of systems auditing in this country.

In 1979, JIPDEC inaugurated a second systems auditing committee, this one chaired by Takehiko Matsuda, then a professor at Tokyo Institute of Technology who later became headmaster of that university, and who is currently serving as headmaster of the Sanno College. This newly formed committee put together a report titled "Guidelines to the Implementation of Systems Auditing," which was published in March 1980. This report stirred up quite a reaction because, in its attempt to promote and

establish systems auditing in Japan, it made recommendations to both government and industry, and formulated a draft proposal for systems auditing criteria. The committee asked four organizations to study these proposals, and to provide it with feedback in the form of opinions/conclusions. The organizations in question were the Japan Certified Public Accountants Association, The Federation of EDP Users Groups, the Japan Auditors Association and the Japan Internal Auditing Association. All four organizations agreed that criteria were necessary in order to promote and establish systems auditing in Japan, and suggested that certain revisions be made to the original proposals to better reflect this.

## SYSTEMS AUDITING CRITERIA

In 1985, the Ministry of International Trade and Industry (MITI) publicly announced its systems auditing guidelines. These guidelines resulted in part from two reports put out by the Information Industry Committee (IIC) of the Industrial Structure Council (ISC), which pointed out the need for the creation of such criteria.

### Proposal For The Establishment Of Systems Auditing

In June 1981, the IIC submitted a report titled "Guidelines to an Affluent Information Society" to the Minister of International Trade and Industry. This report, a gist of which follows, called for the establishment of systems auditing in Japan.

The report claimed that systems audits are a powerful means of ensuring the security of computer systems. It claimed that systems audits are designed to assure the efficiency, reliability and security of computer systems, and are therefore conducted by independent auditors based on set standards (systems auditing criteria). The auditor thoroughly inspects and evaluates the computer system, and then reports his findings, complete with advice and recommendations, to the owners/operators of the system. Systems auditing cannot absolutely assure the security of a computer system, it admitted, but it can contribute greatly to avoiding system errors and downtime, to protecting secrets and preventing computer crime.

Computer systems come in various sizes and configurations, depending on what companies or organizations are using them. The report stated that it is therefore extremely difficult to formulate uniform systems auditing standards capable of being applied across the board, i.e. to numerous different companies and/or organizations. And auditors must be knowledgeable not only of computers and computer systems, but also of accounting work and processes, it pointed out. This being the case, the report concluded that Japan still has a long way to go before it can establish a viable systems auditing system.

However, the report predicted that as the impacts of computer system malfunctions and downtime become more widespread in future, the realization of the need for systems auditing can be expected

to grow, not only within companies and organizations, but throughout society.

The report urged the government to act rapidly to set down guidelines for systems auditing standards, to establish training programs for auditors and related personnel and to formulate other measures deemed necessary for the establishment of systems auditing in Japan.

## Proposal For Formulating Systems Auditing Criteria

In December 1983, IIC submitted an interim report to the Minister of International Trade and Industry containing the findings of its Security Measures Subcommittee on computer security. One of the recommendations put forth in this report was that the government formulate systems auditing criteria.

This report stated that as of the time of its preparation only about ten percent of all Japanese companies were using systems audits. It also pointed out that there was a significant difference in the occurence of malfunctions and downtime between those firms that were employing systems audits and those that were not (The average time between downtime and the average length of each downtime worked out to 530 hours and 50 minutes, respectively, for those firms employing systems audits, but worked out to 450 hours and 75 minutes, respectively, for those firms that were not performing systems audits.). The report advised that there was a need to promote the introduction and use of systems auditing in Japan. It stressed that systems auditing should be central to any guidelines put forth regarding computer security to ensure that security measures are implemented to their fullest.

In more specific terms, the report suggested that the government should set forth guidelines regarding the conduct of systems auditing, and should make these guidelines public. At the same time, the government should also take steps to introduce a systems auditing examination into the information processing engineers examinations then in existence to promote the training of systems auditors, the report advised.

## Announcement Of Systems Auditing Guidelines

Based on the interim report it received in December 1983 from IIC, MITI set up a Systems Auditing Subcommittee within its Informatization Measures Committee in June 1984, and through this subcommittee set about putting together guidelines for systems auditing. These guidelines were formally announced in January 1985.

These guidelines consisted of three types: general criteria (13 provisions); implementation criteria (105 provisions); and reporting criteria (9 provisions).

The general criteria stipulated the basic objectives and targets of systems auditing, as well as qualifications for systems auditors, the frequency/times at which they should be performed, how to plan systems audits and systems auditing procedures. The implementation criteria set forth rules that coincided with

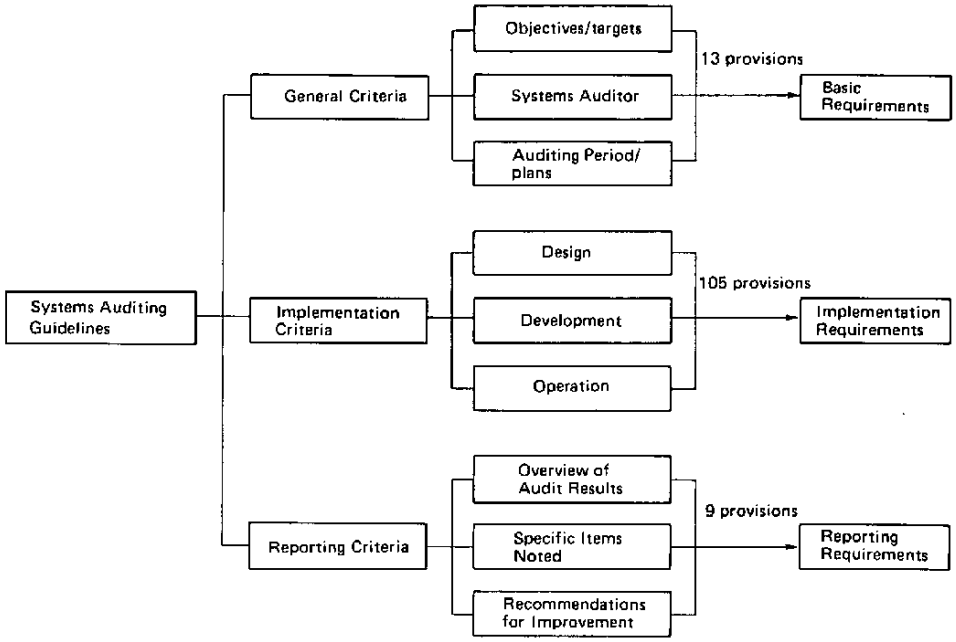


**Figure 1. Outline of Systems Auditing Guidelines**

the design, development and operation of computer systems for systems auditors to follow when performing auditing. And finally, the reporting criteria set down by MITI stipulated those items that had to be incorporated into reports of audit results, as well as the types of measures that should be recommended based on those results.

MITI is striving to promote the widespread use of these systems auditing guidelines in conjunction with its computer system security guidelines announced back in 1977 (revised in 1984) as a basis for measures designed to improve computer system security and reliability. Neither of these guidelines are binding, but rather are being promoted by MITI as suggested guidelines.

Following the announcement of these systems auditing guidelines, JIPDEC, with the cooperation of MITI, published a systems auditing guidelines manual that explained each of the 127 provisions contained in the guidelines in detail. This manual has become the "bible" for systems auditing criteria in Japan.

## CURRENT STATE OF SYSTEMS AUDITING IN JAPAN

According to the results of a survey conducted recently by JIPDEC, the ratio of Japanese firms implementing systems auditing in 1987 worked out to just 19.4%, which is still quite low.

## Systems Auditing By Size Of Information System

Only 19.4% of all Japanese companies are currently using systems auditing. However, if we break this figure down by size of computer system, we see that a high 61.9% of those users of very large-scale systems who responded to the survey are employing systems auditing. It is felt that in the not too distant future, all very large-scale computer system users will carry out systems audits. When it comes to large-scale computer systems, only 28.3% of the users of this size category are utilizing systems auditing. This is too low a percentage. Between 70–80% of the users of this class of computer system should commence performing systems audits as soon as possible (See Table 1).

## Ratio Of Firms Employing Systems Auditors

Only a scant 5.7% of all Japanese firms employ systems auditors to carry out systems auditing. Therefore, of the 19.4% of Japanese firms performing systems audits, less than one-third that percentage are doing so under the expert guidance of trained systems auditors. This shortage of systems auditors is the biggest single problem facing systems auditing in Japan today (See Table 2).

## Systems Auditing By Stage of System Operation

One part of the JIPDEC study was aimed at determining which stage of system operation – design, development or operation – was subjected to systems auditing the most. The results of the study indicated that systems audits are performed on 16.8% of information systems in the design stage of operation; on 36.6% in the development stage; and on 95.3% of information systems in the operation stage. Thus, systems audits in Japan are overwhelmingly aimed at information systems already in operation. However, systems audits conducted on systems under development seem to be on the increase recently (See Table 3).

## Points Focused on During Systems Audits

Respondents to the JIPDEC survey stated that the major points focused on during the performance of systems audits are reliability (85.7%), security (73.0%) and privacy (60.3%). If we compare the replies of those respondents from secondary and tertiary industries, we see that members of tertiary industries are employing systems audits for security, reliability and profitability, in that order. This can be attributed to the fact that the computer networks in use in the tertiary industries are larger and more extensive than those employed by members of the secondary industries (See Table 4).

## SYSTEMS AUDITORS EXAMINATION SYSTEM

Following the release of its systems auditing guidelines, MITI, in December 1985, announced the establishment of a

**Table 1. Systems Auditing by Size of Information System**

| Computer Categories \ Systems Auditing Experience | | Yes | No | Total |
|---|---|---|---|---|
| Very-large-scale | No. of Firms | 26 | 16 | 42 |
| | % | 61.9 | 38.1 | 100.0 |
| Large-scale | No. of Firms | 78 | 198 | 276 |
| | % | 28.3 | 71.7 | 100.0 |
| Medium-scale | No. of Firms | 64 | 379 | 443 |
| | % | 14.4 | 85.6 | 100.0 |
| Small-scale | No. of Firms | 17 | 139 | 156 |
| | % | 10.9 | 89.1 | 100.0 |
| Very-small-scale | No. of Firms | 0 | 33 | 33 |
| | % | 0.0 | 100.0 | 100.0 |
| Small Business Computers | No. of Firms | 0 | 1 | 1 |
| | % | 0.0 | 100.0 | 100.0 |
| Minicomputers | No. of Firms | 0 | 5 | 5 |
| | % | 0.0 | 100.0 | 100.0 |
| Others | No. of Firms | 0 | 0 | 0 |
| | % | 0.0 | 0.0 | 0.0 |
| Total | No. of Firms | 185 | 771 | 956 |
| | % | 19.4 | 80.6 | 100.0 |

(Note: The values attributed to each size category are given below.

| No. | Size Category | | Purchase Price | Monthly Rental Fee |
|---|---|---|---|---|
| 1 | General-purpose Computers | Very-large-scale | 1.5 billion yen or more | 33.33 million yen or more |
| 2 | | Large-scale | Between 250 million and 1.5 billion yen | Between 5.55 million and 33.33 million yen |
| 3 | | Medium-scale | Between 40 and 250 million yen | Between 880 thousand and 5.55 million yen |
| 4 | | Small-scale | Between 10 and 40 million yen | Between 220 and 880 thousand yen |
| 5 | | Very-small-scale | Between 5 and 10 million yen | Between 110 and 220 thousand yen |
| 6 | Small Business Computer | | | |
| 7 | Minicomputer | | Minicomputers are generally used as dedicated machines. | |
| 8 | Others | | These computers fall outside the above cited categories. | |

**Table 2. Ratio of In-house Systems Auditors**

(Upper figures: no. of companies; lower figures: percentages)

| Systems Auditors / Industry | Exist | Do Not Exist | Total |
|---|---|---|---|
| Primary industries | 0<br>0.0 | 4<br>100.0 | 4<br>100.0 |
| Secondary industries | 20<br>4.8 | 396<br>95.2 | 416<br>100.0 |
| Tertiary industries | 35<br>7.2 | 452<br>92.8 | 487<br>100.0 |
| Public sector | 0<br>0.0 | 51<br>100.0 | 51<br>100.0 |
| Industry-wide Total | 55<br>5.7 | 903<br>94.3 | 958<br>100.0 |

**Table 3. Systems Auditing by Stage of System Operation**

(Upper figures: no. of companies; lower figures: percentages)

| Stage of Operation / Industry | No. of Responses | Design Stage | Development Stage | Operation Stage |
|---|---|---|---|---|
| Primary industries | 1<br>100.0 | 0<br>0.0 | 0<br>0.0 | 1<br>100.0 |
| Secondary industries | 99<br>100.0 | 13<br>13.1 | 28<br>28.3 | 94<br>94.9 |
| Tertiary industries | 89<br>100.0 | 19<br>21.3 | 42<br>47.2 | 85<br>95.5 |
| Public sector | 2<br>100.0 | 0<br>0.0 | 0<br>0.0 | 2<br>100.0 |
| Industry-wide Total | 191<br>100.0 | 32<br>16.8 | 70<br>36.6 | 182<br>95.3 |

**Table 4. Aspects Focused On During Systems Audits**

(Upper figures: no. of companies; lower figures: percentages)

| Points Stressed / Industry | No. of Responses | Security | Reliability | Privacy | Conformity | Profitability | Timeliness | Productivity |
|---|---|---|---|---|---|---|---|---|
| Primary industries | 1<br>100.0 | 0<br>0.0 | 1<br>100.0 | 0<br>0.0 | 0<br>0.0 | 0<br>0.0 | 0<br>0.0 | 0<br>0.0 |
| Secondary industries | 98<br>100.0 | 64<br>65.3 | 86<br>87.8 | 44<br>44.9 | 36<br>36.7 | 14<br>14.3 | 23<br>23.5 | 15<br>15.3 |
| Tertiary industries | 88<br>100.0 | 73<br>83.0 | 74<br>84.1 | 69<br>78.4 | 34<br>38.6 | 23<br>26.1 | 21<br>23.9 | 10<br>11.4 |
| Public sector | 2<br>100.0 | 1<br>50.0 | 1<br>50.0 | 1<br>50.0 | 0<br>0.0 | 1<br>50.0 | 1<br>50.0 | 1<br>50.0 |
| Industry-wide Total | 189<br>100.0 | 138<br>73.0 | 162<br>85.7 | 114<br>60.3 | 70<br>37.0 | 38<br>20.1 | 45<br>23.8 | 26<br>13.8 |

national-level equivalency examination for systems auditors. This announcement also carried with it the implied meaning that MITI was taking a direct interest in the cultivation of systems auditors. The new examination was called the Information-Technology Systems Auditors Examination, and was incorporated into the existing Information-Technology Engineers Examination system.

The first systems auditors exam was given in October 1986. A total of 10,699 individuals applied to take the test, of which 6,767 actually sat for it. Only 425 of these people passed the exam. This exam is now given on the third Sunday in October every year.

## Qualifications And Level Of Expertise Required For The Exam

The Information-Technology Systems Auditors Examination is aimed primarily at persons engaged in the conduct of systems auditing. Applicants must be 27 years-of-age or over, must possess general knowledge equivalent to that of a college graduate, should have five or more years general working experience, must possess specialized knowledge related to the design, development, operation and auditing of information systems, and must be capable of performing a systems audit.

## Areas Tested

The subject matter tested by the Information-Technology Systems Auditors Examination can be categorized into the following four areas:

1) Knowledge of the configurations and functions of information systems;
2) Knowledge of information system design, development and operation;
3) Skills related to systems auditing; and
4) Other related knowledge.

### Testing Methods And Time Limits

The exam is divided into three parts: a 150-minute multiple choice exam; a 90-minute short-answer exam; and a 120-minute long-answer exam. The examination begins at 9:30 AM and finishes at 4:50 PM.

## SYSTEMS AUDITING CONSULTATION SERVICE

In 1986, JIPDEC started up a Systems Auditing Consultation Service to provide firms encountering problems in the course of introducing systems auditing into their operations, and to help promote the further spread of systems auditing in Japan.

Companies experiencing problems in introducing and/or implementing systems audits in their operations can come to JIPDEC to receive consultation from a member of the Systems Auditing Promotion Committee, which is made up exclusively of systems auditing specialists. This service is free of charge.

## SYSTEMS AUDITING SOCIETY

A Systems Auditing Society was founded in March 1987. The chairman of this society is Takehiko Matsuda, former president of Tokyo Institute of Technology, who is now serving as president of the Sanno College. The goals of this society are to promote the exchange of information and research results concerning systems auditing between and among members of the society, and to contribute toward the development of a sound information society through the conduct of scientific research and investigations.

### Major Activities

#### Systems auditing committee

The Systems Auditing Committee of the Systems Auditing Society was set up to study how best to match systems audits up with the way Japanese firms do business, and to establish systems auditing theories.

#### Monthly research meetings

The Systems Auditing Society also holds meetings once a month to provide members with a forum to announce the results of their work and/or to exchange ideas and information.

#### Risk management group

The Society also put together a Risk Management Group to carry out basic research on risk management to deepen members' understanding of this area.

#### Systems auditing techniques group

The Systems Auditing Society set up a Systems Auditing Techniques Group to study the various techniques used in auditing information systems. By so doing, the Society hopes to further its members' understanding of the functions, applicability and utilization methods associated with systems audits.

**Computer crime group**

The Society also sponsors a Computer Crime Group. This group studies computer crime from the standpoint of the systems auditor, analyzing and defining the processes involved so as to find ways of preventing computer crimes, or at least of detecting them early.

**Consulting group**

Systems auditing consulting is a popular new business which is still not well understood. The Systems Auditing Society's Consulting Group, therefore, conducts research on what systems auditing consultation should be all about, and how it should be carried out.

## Membership Qualifications

Prospective members of the Systems Auditing Society must possess the following qualifications:

1) They must be experienced in the field of systems auditing;
2) They must be systems auditors working for a company;
3) They must be intent on studying systems auditing while engaged in information processing or auditing work; and
4) They must be approved by the Society's board of directors.

# CURRENT NEWS

## NTTI DEVELOPS NEW TELE-COMPUTING SYSTEM

Nippon Telegraph and Telephone International Corporation (NTTI) has developed a new telecomputing system called "PC Network," which features international file transmission functions that are only about half as expensive to use as VENUS-P, Kokusai Denshin Denwa Co., Ltd.'s international public data transmission service. The company plans to begin marketing the system in earnest later this fall.

This new PC Network system makes use of JUST-PC adaptors to interconnect personal computers (PCs) installed at user companies' headquarters, branch offices and overseas business locations, thus creating an in-house network, and, with the help of international telephone lines, an inexpensive two-way file transmission system. JUST-PC adaptors employ the telecommunications system recommended by the Ministry of Posts and Telecommunications (MPT).

The transmission rate (speed) of the PC Network is 4,800 bits per second (bps), which is considerably faster than the 1,200 bps capable with VENUS-P. PC Network employs the popular HDLC data transmission protocol, and, in addition to Japanese- and English-language files produced via word processors, can also handle dBase and a variety of other data file transmissions. User IDs and passwords ensure the security of the system.

According to NTTI's calculations, users of PC Network will be able to transmit an amount of data equivalent to that capable of being printed on 10 sheets of A4-size paper (letter-size paper) between Japan and the United States for 460 yen. It costs 870 yen to transmit the same amount of data from Japan to the U.S. using VENUS-P; 3,100 yen using G-III facsimile systems, and as much as 27,000 yen using international telex systems.

Any and all makes and models of PCs currently on the market can be hooked up via the PC Network system.

## JAICI OFFERS TRANSLATION SERVICE SPECIALIZING IN PATENT, SCIENTIFIC AND TECHNICAL DOCUMENTS

The Japan Academic Information Center, Inc. (JAICI) has started up a new service designed to provide timely trans-

lations of information contained in Japanese patent, scientific and technical documents to overseas users upon request. This new service is linked up with two worldwide scientific and technical document database services based in the United States, DIALOG and STN International. Orders for information are received online from these U.S.-based database services via an international network, and translations of requested information are then provided to the end users either via facsimile transmissions or air mail.

Called "JAICI Express Translation Service," this service provides translations of official patent reports and various published academic papers into English, German, French and Spanish in accordance with overseas requests.

Requests for information are sent to JAICI online via the host computers of DIALOG and STN International. Specialists then quickly translate pertinent reports and/or papers and send that information back to the requesting party. When facsimile transmissions are used, the end user can have the information he needs within three days of ordering it.

Only a very few patent and/or scientific and technical online databases contain full text information, most being either bibliographic and/or abstract databases. JAICI's Express Translation Service, however, provides users with rapid, complete translations of full text documents.

Database users are not the only ones who can avail themselves of this JAICI service; orders for information can be placed directly with JAICI via facsimile. JAICI translations ordered online through DIALOG cost anywhere from 90–165 dollars per page, and can be sent to the requesting party via facsimile for an additional 3–5 dollars per page.

## FUJITSU ANNOUNCES NEW AI SYSTEM

Fujitsu Limited announced a new artificial intelligence (AI) system called "KSA Knowledge Information System" on July 9, 1987. This system provides AI-related products via an architecture that is the same whether it is run on personal computers (PCs) or supercomputers, and is designed to develop the AI market across the board, from R&D systems to service-oriented systems.

The KSA Knowledge Information System conforms to Fujitsu's new expert system development support system "ESHELL/X," as well as to its Systems Integration Architecture (SIA) announced before AI languages such as Prolog and Lisp came out. This system is provided with the same specifications whether it is used on Fujitsu's FMR PCs, its M series of general-purpose machines or its VP series of supercomputers. Various other types of applications software are provided through this system, to include performance monitoring and network diagnostic expert systems.

Fujitsu is the first company in the world to come up with this type of AI system, which it plans to incorporate into its next generation computer architecture. In future, Fujitsu hopes to apply this new system to general-purpose telecommunications and office automation, thereby

strengthening the merger of these two fields.

## DISTRIBUTION DATA SERVICE GOES COMMERCIAL

A distribution data service that brings together sales information gathered via retailers' point of sales (POS) systems for use by manufacturers and wholesalers has been commercialized. Since April 1987, the Ministry of International Trade and Industry (MITI) and the Distribution System Development Center have been promoting the development of this service, which collects information from some 200 retailers nationwide and provides it to 13 information service businesses, a portion of which have started marketing that information. MITI plans to increase the number of participating retail stores as well as the amount of data gathered, to cultivate additional information service vendors and to expand this service until it is capable of utilizing all POS data nationwide.

## YAMAICHI SECURITIES PLACING LARGE ORDERS FOR WORKSTATIONS

Yamaichi Securities Co., Ltd. has begun placing large orders for high-performance 32-bit workstations which will serve as the work horses of a third online system it has decided to construct to provide each of its offices with multitasking distributed processing capabilities. The goal is to have the entire system operational by early 1990. The detailed design plans call for 10 nodes to be established nationwide and interconnected via a high-speed packet-switched network. Yamaichi plans to equip each of its offices with local area networks (LANs), and to purchase the terminal processors necessary for distributed processing, plus a large number of 32-bit multitasking workstations equipped with both business and investment information functions.

## Back Issues of Japan Computer Quarterly are as follows:

No. 70: The Informatization of Small and Medium Businesses
69: Expert Systems in Japan
68: Large-scale Projects in Japan
67: Information Services in Japan
66: IC Cards – Cards with Brains –
65: Database Services in Japan
64: Machine Translation – Threat or Tool –
63: EDP Certification – ExamLand, Japan –
62: Liberalizing Telecommunications
61: VIDEOTEX: A Glimpse of The 21 Century
60: The Day of the Robot
59: Financial Revolution – Electronic or Plastic –
58: The Advanced Information Society – ISC Interim Report –

No. 57: The PC Phenomenon
56: Information Services Japan '83
55: Electronic Money
54: Online Systems
53: Computer Literacy
52: Personal Computer
51: Database Service in Japan
50: Industrial Robots
49: International Conference on Fifith Generation Computer Systems
48: General Survey
47: Office Automation
46: Microcomputer Industry
45: 1980 Trends in Japan's Computer Industry
44: Distributed Database System JDDBS-I
43: Systems Audition Standards

## ORDER FORM

FUJI CORPORATION
HAN-EI NO-2 BLDG. 6F.
1-10-1 SHINJUKU SHINJUKU-KU,
TOKYO 160 JAPAN.
TEL.(03)350-8701 TELEX:02425496 FUJICO J

Yes, Please Rush Me The Items Checked Below:

☐ Japan Computer Quarterly (Quarterly)

☐ Annual Subscription $85

☐ Single Copy No. _____ $22 per copy
_____
_____
_____

Total : $ _____

Name _____ Title _____

Company _____

Address _____

☐ Check enclosed
☐ Bill me


Japan Information Processing Development Center