情報産業における秘密保護

中間報告書

昭和44年4月

財団法人　日本情報処理開発センター
財団法人　日本経営情報開発協会

序

本書は、当財団が、財団法人　日本経営情報開発協会および日本ＥＤＰ株式会社に委託した「情報処理ネットワーク形成における秘密保護問題の調査」に関する中間報告書である。

財団法人　日本情報処理開発センター

会長　難　波　捷　吾

調査にあたって

予想以上に急速なコンピュータの普及と、その高性能化は、ソフトウェア開発技術の進歩と相俟って、情報化社会の実現へ急テンポで歩を進めつつあります。さらにコンピュータと通信回線との結合は、コンピュータの高度利用に画期的な新生面を開き、情報処理能力も飛躍的に向上し、新しい産業分野としての情報産業が大きな期待のもとに抬頭の兆しを見せております。

すでに情報処理サービスを業とするものは数百に達し、情報提供サービスも急速に発展する気運を示しております。ことにデータ・バンクの発達による個人の人事情報システムや、信用調査業務の出現によって、情報処理に伴なう秘密保護の必要性が重大な関心を呼び起こして参りましたのも当然のことと思われます。

当協会は、通商産業省・産業構造審議会・情報産業部会の審議に資するため財団法人情報処理開発センターの委託をうけて、各分野における学識経験者による調査委員会を設置し、必要な対策について協議を重ねました結果、ここに中間的な取りまとめを行ない、報告書を作成いたしました。

わが国では未だコンピュータ間の連携をもった大規模なシステムは実現していない現実の状況から見ますと、この報告書はやや時期尚早の感がないでもありません。しかしながら、近い将来確実に迎えるべき情報化社会の問題を捉えてこれに備えることは、極めて重要なことと信じます。

委員諸氏のご努力を謝するとともに、こんごさらに一層のご研究により、将来の方向を解明されることを期待しております。

財団法人　日本経営情報開発協会

理事長　平　田　敬一郎

情報産業の秘密保護に関する調査委員会

委　員　氏　名

（五十音順）

委員長	大野達男	野村電子計算センター㈱・副社長
委　員	飽田了三	コンピューターシステム㈱・常務取締役
	伊藤憲太郎	日産自動車㈱・総務部次長
	大久保茂	㈱コンピュータアプリケーションズ・社長
	金岡幸二	日本計算センター協会・会長
	栗田昭平	日本電子計算機㈱・調査室長代理
	鈎木秀郎	日本郵船㈱・機械二課長
	田川行三	㈱三井銀行・事務部長
	中島朋夫	日本ＥＤＰ㈱・専務取締役
	西岡宏治	日本経営情報開発協会・事務局次長
	堀口瑞典	日本アイ・ビー・エム㈱取締役広報部長
	松井稔	行政管理庁、副管理官
	山中広	㈱日通総合研究所・取締役
	若曾根和之	通産省重工業局情報産業室・課長補佐

目　　次

付　属　資　料

参　考　資　料

I. 情報産業における秘密保護の必要性

1. 社会の発展と秘密保護との関連

これまで個々の企業または官庁において独立して使われていた情報処理システムが、回路技術および利用技術の急速な発展と時代の要請にしたがって複数のシステムが互いに関連をもって働くようになり、また通信回線を介して遠隔地から不特定多数者が利用できるようになってきた。

したがって、そこで蓄積され処理される情報が、互いに有機的に関連を持つことが可能になるに及んで、情報化社会の秘密保護の問題と個人生活に及ぼす影響が大きな問題としてクローズアップされてきた。とくに加速度的に進歩する情報処理技術と急激に変化する社会の現状を見るとき、情報化社会の到来は想像以上に間近いとも考えられ、なおさらその重要性が大きくなりつつある。

先進諸外国においても近年これらの問題についての議論が活発化しさまざまな研究が行なわれているが、わが国でもこれとペースを同じくして情報産業の抬頭に附随する問題を把え、世論の喚起をうながすことは極めて有意義なことと思われる。

もちろん情報化社会の包含する問題とそれに対処するための必要な社会改革の議論は単に情報産業にたずさわるもののみならず、学者、政治家、法律家、倫理学者、宗教家にも包含する大問題であり、短時日に結論の出せる問題ではない。

しかしこの報告書は、そこに包含される問題と対策についてその輪郭を浮彫にするとともに、とくに情報産業にたずさわるものの立場から秘密保護にたいする技術面をもカバーすることにより、こんごの情報産業全体の理想的な発展とコンピュータの有効な利用に少なからず示唆を与えるものであると信ずる。

2. 情報社会において秘密保護が必要とされる社会的背景

赤外線カメラ、テープレコーダー等の発明に例をとっても、機械文明の進展は、多くの場合そのもたらす恩恵とは裏腹にプライバシーへの脅威という問題を併存して今日に至っている。しかもこれら機械の普及につれてその価格は次第に低廉となり、プライバシーの侵害をそれだけ容易なものとしてきた。

２０世紀最大の技術革新といわれる情報処理システムの発達も、取り扱う対象が情報であるだけにこれまでになくその影響は大きく、また多くの問題を社会に投げかけることは想像に難くない。

情報蓄積の規模が大きくなり集中化が進むにつれてその利用価値はますます大きくなることは当然であり、情報蓄積の必要性は社会科学、流通産業、雇傭労働関係、警察、教育、福祉更生とあらゆる分野に認められている。

ことに高性能コンピュータの出現と、ソフトウェア開発技術の進歩は従来とうてい不可能であった情報の山の中から意味のある関連性を見出し、詳細な統計上の分析評価を行なうことを可能とし、社会・経済の動きにたいし鋭い洞察力を駆使するための手段を提供した。

例えば都市機能の膨脹と人間の行動範囲の拡大に対応して地方行政機関は変化と動向を適確に把握し必要な対策を立て、タイムリーに行動を起すことができるようになった。

情報処理システムを交通管制、雇傭問題、流通社会、福祉問題等に利用する場合その利用効果は計りしれないものがある。

3. 機密情報の限界・範囲

しかし一方、情報処理システム利用の恩恵とは逆に情報処理システムの巨大な能力が情報化社会において個人および企業に不安と脅威をもたらす可能性をもつものであることも否定できない。

現状においては必要な情報が必ずしも完備されておらず、例え入手可能であったとしても、それらの情報が互いに相関関係なしに散在するため独立した情報を互いに有機的に集合させ関連づけるにはかなりの労力と時間を必要とする。したがって情報の分散は情報の秘密性にたいする一種の保護作用として働いているという見方もとることができる。

しかし確実に将来到来するであろう情報化社会においては企業、政府機関および個人に関する一連の情報は組織的に蓄積され、常に秘密の漏洩と悪用の不安にさらされることになる。とくに、情報処理システムの利用とデータバンクの設立は、万一運用を誤ると圧制の道具ともなりかねないことを認識しなければならない。

両刃の刃ともみられる情報処理システムの特質を認識し、理想的情報化時代を実現するためには、大衆の理解、安全策としての技術開発、企業活動の基準の再検討、政治、法律、倫理面の改革が必然となるだろう。

Ⅱ　海外における秘密保護の状況

今までに入手し得た米国および英国の文献によれば、両国の「情報の秘密保護」に関する問題は、基本的に変りはない。いま、両国の文献から、コンピュータ発展に伴なう情報の秘密保護をめぐる基本的態様を要約すれば、つぎのようになろう。

1. 情報の蓄積形態

コンピュータ出現以前にも、情報の蓄積は、国の各種情報ファイル、地方公共体における住民情報ファイル等々、枚挙にいとまがないほどの実例があった。しかし、これらのファイルは、相互に連係がなく、しかも、情報検索能率は、極めて低かったということができる。コンピュータは、こうしたファイルの検索能率を飛躍的に向上せしめるばかりでなく、情報流通の広域化を促がしつつある。さらに、大容量記憶機能は、従来、全く考えられなかったスケールで、各種の情報を少数箇所に集中せしめることを可能にする。ここにデータ・バンクあるいは、情報処理サービス業における情報ファイルの利用の活発化という現象が生じた。

情報システムは、統計情報システム（statistical information system）と個別情報システム（intelligence information system）に二大別できる。前者は、個別情報を整理し、同一特性をもった集団に関する諸特徴（たとえば、××地域の住民のうち年収：１００万円以下の者は、その地域人口の何％か）を出力するシステムであり、後者は、個別実体の生まのデータを検索、編集、出力する（たとえば、○○氏　の収入は××万円）システムである。

これら二大システムは、人間生活と産業活動にとって、必要なものであり、それらの情報蓄積形態は、およそ次頁のように分けることができよう。

このように、情報蓄積主体は、政府、地方公共体、業界団体、民間企業、

情報システムの例

情報蓄積主体	種類	統計情報システム	個別情報システム
政府（行政）	個人情報	国勢調査ファイル	運転免許ファイル 労働市場資源ファイル 犯罪者ファイル 健康保険ファイル 個人納税ファイル
	公的情報	生産統計，貿易統計， 犯罪統計 （マクロ経済統計）	判例検索システム 特許検索システム 企業財務（有価証券報告書ファイル），企業納税ファイル
地方公共体	個人情報	人口統計ファイル	住民登録ファイル 地方税納税ファイル
	公的情報	産業統計ファイル	土地台帳ファイル
業界団体 民間企業	個人情報		医療ファイル 個人信用ファイル（クレジットカード会社，生命保険会社，銀行等）
	公的情報	産業，統計ファイル（協会等） 科学・技術情報ファイル	企業財務計数ファイル（銀行，保険会社，調査会社等） 株価情報ファイル 座席予約システム
情報処理企業 情報提供企業	個人情報	市場調査ファイル	
	公的情報	科学・技術情報ファイル 社会情報（ニュース）検索システム 産業統計	旅行情報システム

情報処理企業、情報提供業と、広範な利用形態が考えられる。

2. プライバシーの保護

秘密保護には、情報の漏洩の防止とプライバシー保護の二つの側面があるが、海外では現在までのところプライバシーの侵害の恐れに関する議論が殆んどを占めているようである。

プライバシーの侵害は、統計情報を供給している限りは、起こらないが、個別情報の供給に際して生じる可能性がある。統計情報システムの場合でも、もし、そこに蓄積されている生まの個別データを第三者に洩らした場合には、プライバシー侵害を惹起し得る。

欧米におけるコンピュータ発展に伴なう情報の秘密保護の問題には、つぎの二つの対立する思想が流れているようである。

(1) 国民の知る権利……米国議会では、一種の〃情報の自由法〃(a freedom of information law)を通過させ、国民に連邦政府が何をしつつあるかを知る権利を与えた。この法律は、①国防に関する書類、②FBIのファイル、③所得税申告書ファイル、④特許出願ファイル、⑤Executive branch memoranda ⑥通商上の秘密および産業財務データ、の6つの情報を除いた、連邦政府のファイルを理論上公開したものである。農務省は、この法律に非常に協力的で、政府補助金5,000ドル以上を受領した農民の人名録を誰にでも閲覧させると発表した。

(2) 個人のプライバシーの保護……個人のプライバシーの擁護は、①一人でいたいという権利の侵害、②通常の礼儀を踏まずに個人的私事を公表すること、③文書を偽造して、ある個人の考えに反することを述べ、誤ったイメージを一般にもたせること、④許可なく個人人格のある要素を商売に利用すること、の4つを行なわせないことでもあると、分析されてきた。

3. 連邦政府の情報集中傾向

政府、とくに連邦政府の情報集中傾向は著るしく、各種情報の全国民、全国的規模の情報集中化は進行しつつある。例えば米国SSA(社会保険

庁）においては、１億7,９００万口座にのぼる健康保険支払業務を行なっており、国民の性別、年令、氏名、給与などの情報を蓄積している。数年以前、学業成績を含め、出生後の個人に関するあらゆる社会歴データを蓄積しようというナショナル・データ・センターの構想が連邦政府から出され、世論の反撃に合い現在ペンディングになっている。これは、政府が余りに強大になり、個人のあらゆる情報を知るようになると、個人の自由が侵される恐れがあると感じたためである。スタンフォード研究所は、現在の法律は、プライバシーの保護規定があいまいで、連邦政府の情報システムが強大化するにつれ、個人のプライバシーが侵される危険は十分にあるといっている。

4. プライバシー侵害の防止策

Harbridge House Inc. のリチャード・Ｉ．ミラー氏（上級コンサルタント）は、データメーション誌１９６８年９月号で、プライバシー侵害の防止策として、つぎのことを提案している。

① 個人データを伝送する通信回線に対して最低限度の暗号化措置を工夫すること。こうすれば、電話の盗聴より技術的に費用がかかるので、データの盗受はしないだろう。

② 個人データは、決して〃直ぐに理解できる状態〃でファイルに蓄積しないこと。

③ プログラマーが故意に、また、不注意に個人データに最短ルートのアクセスを行なうことができないプログラムが、データ・バンクに用意されているかどうかを、銀行記録の監査と同様に標準化し、監査すること。

④ 個人データの照会がどこから発せられたか、その源を検知し、記録する装置をコンピュータに内蔵させること。

5. 事　例

プライバシー侵害には、知らないうちに機械的に発生する場合と、故意に行なう場合とがあるが、今後の可能性の事例をあげれば次のとおりである。

（例１）　信用調査会社に個人信用データのファイルがある。ある商社が、カストマーへ商品を配送したが、彼はそれが注文のものと違うので、受け取らず、支払も拒否した。ところが、代金を支払わなかったという事実は、そのままデータ・バンクに記録され、１年が経過した。彼は、ある店で買物をしようとして、クレジット・カードを差し出すと、彼は、１年間代金を支払わなかった人物として、品物の販売を拒否される恐れがある。

（例２）　今後１０年以内に、事業主に幹部社員およびその見込者の信頼度、忠実度、交友関係、恋愛関係、財産、身分、経歴を調べ、蓄積する機関ができ、企業に情報を有料で提供する可能性がある。その機関は、コンピュータ・システムを利用してあらゆる個人情報を容易に入手するようになるだろう。ごく一部でも、間違った情報や歪められた情報が蓄えられたならば、それによって起る被害を考慮しなければならない。

（例３）　ロックフェラー財団のロバート・モリソン博士は、「われわれは、組織化された知識が、それを得ようと骨を折っている人びとの手中に、広大な力（権力）を与えることを認識する時点に至りつつある」と述べている。確かに、われわれは、情報は力なりという事実を見聞している。個人に関する各種の記録は、いまや数十億という数に達している。われわれは生まれた瞬間から、出生、両親の納税額、収入、持家、負債、学業、成績、ＩＱ、性生活、性格その他もろもろのデータの収集・記録が、各種の公的、私的機関によって行なわれている。連邦政府が、個人である市民の情報を中央センターまたは複数センターへ集中するという計画を許した場合は、個人の自由が侵害される危険が明らかに存在すると考える。

（Vance Packard 氏の１９６６年における米議会公聴会における陳述意見の一部から）。

（例４） １９６８年におけるカリフォルニア州議会の議決にもとづき、政府間ＥＤＰ委員会（an Intergovernmental Board on Electronic Data Processing）が設置された。その機能は、同州内の地方政府間のデータ処理システムの運用に関するポリシーを確立することにある。同委員会は、最初の活動として、〃プライバシーおよび機密分科会〃、を設け、コンピュータによって惹起されるプライバシー問題を処理することにした。

つぎにあげるのは、同分科会の目的である。

(1) 政府機関のファイルに記録され、また伝送される記録のうち、個人等の情報に関してそのプライバシーを維持し、法によって保護を規定されている情報（個人情報および企業等の組織に関する情報）の安全を守るポリシーを勧告する。

(2) 各種の管理技法、利用できる法令、技術方法および倫理基準の採用を通じて、ＥＤＰ設備に蓄積されている情報を管理するガイドラインを作成し、委員会に提出する。

(3) 下記組織との連絡を密にする手段を勧告する。

ａ）現在、計画・開発中の機密安全装置を機械に内蔵するようコンピュータ・メーカーを刺激すること。

ｂ）地方政府のあらゆるレベルにおける情報を保護する活動を調整する。

ｃ）たとえば、教育機関、データ処理機関、コンピュータ科学者など、同様の目的をもっている政府以外の組織と個人との連絡をとる。

(4) ＥＤＰ設備に関連して起こるプライバシーおよび秘密事項の法規のリコメンデーション。

(5) 上述の諸目的の強力な追求のために、政府の情報の必要条件に応える部門を維持する。

(6) 少なくとも毎年、上述の諸目的を反省し、その達成状況を報告する。

Ⅲ　国内における秘密保護の現状と問題点

1.　情報処理産業に於ける秘密の実情

情報処理産業に於いて、「取扱う秘密は何か」という事に非常に問題がある。

「プライバシーを侵害するおそれのあるデータ」

「国家等権力の統制を助成する可能性あるデータ」

「企業機密」

「国家機密」

等々のデータと、

「企業運営・国防運用等のシステム、或いはソフト・ウエア」

等のシステムと考えられているのが通説である。具体的に、どのデータ、どのシステムが秘密であるかは、

(1)　過去の経験よりの常識的認定

(2)　当事者と、情報処理企業との間の契約による

にまたなければならない。

後者のように、契約により「これこれのデータ」、又は「システムのこの範囲」が秘密であると文章により明確になっていれば、秘密保護上、対象が把握しやすい。然し、現実には秘密の対象物が極めて漠然とし、過去の経験より常識的に判断しており、その解釈について紛争の種となるおそれのあるのが実情である。

例えば、刑法第１３４条の秘密漏泄に対する罰則に於いても、「故なく其業務上取扱いたることについて知り得たる秘密」とあり、秘密とは何かとの定義はない。又、国家公務員法第１００条、地方公務員法第３４条においても、「職務上知る事の出来た秘密」とあり、刑法同様、秘密の定義はない。統計法第１４条に於いても、「人、法人又はその他の団体の秘密に属する事項」とあり、これも前述同様である。

民間各社に於いても、秘密保護上、秘密の定義を明確にしているところは少ない。例えば、就業規則上、秘密保持条項はあっても、秘密の定義を明確にしてあるものはないといってもよい。即ち、「業務上の秘密を他にもらさない」（北陸電力就業規則第4条）「経営上の機密若しくは業務上知り得た機密をもらさない」（富山計算センター就業規則第11条）等となっている。

然し、就業規則上ではなく、文書規定等に企業機密について、(秘) (極秘) 等々のランクづけをし、その印のついた書類の取扱いについて、具体的に定めている企業は多いし、又、今後その傾向にある。

秘密は、「どの事項がそれに該当するのか、又、その取扱いをどうするか」を定めないで、秘密保護問題を語ることは、全く砂上の楼閣である。

秘密問題の更に複雑な事は、A企業で秘密でないデータが、情報処理産業に入手され、そのデータを利用することにより、B企業の秘密とする事に抵触し、又は、プライバシーの侵害になる事があり得ることである。

この問題は、個別企業内・個別官公庁内での秘密保護問題以上にやっかいな特殊性のある事を示している。情報処理産業に於ける秘密保護問題は、他企業の秘密保護問題とことなるのはこのように、データの集積が生じ、それが自動的な力をもつ可能性のある点である。従って、秘密の定義、データ・システムの取扱い法について特別な配慮が必要であろう。

2. 企業基盤・信用と秘密保護

情報処理産業が、秘密の保持を重大な問題であるとし、それに努めている事は事実である。然しながら、それらが好むと好まざるとにかかわらず、秘密保護を困難にする場合がある。それは、企業であるという宿命からであるが、まれなケースでもあり、それを防止する方法を講じなければならない。

(i) 企業倒産

企業基盤の薄弱な情報処理産業の営業が困難となり、倒産又は、これに準じた状態に陥った場合、当然、債権者の意向が絶対となる。この場合、その企業の有する秘密たるべきデータ・システムがどの様に処理されるか不安がある。

ただし、米国に於いて、数年前まで計算センターの新陳代謝が年50%に及んだときも、又、日本に於いて、計算センターの倒産の生じたまれなケースの時も、秘密漏洩問題が生じていない事は社会の良識の故であり、必配は杞憂にすぎないかもしれない。

(ii) 営業上の圧力

企業基盤が薄弱であり、その上、経営者のモラルの低い場合、その企業の存立を危うくするような、営業上の圧力が加った時、秘密保護が困難になるケースがあると想像できる。

以上の2つのケースは、極めてまれなケースではあるが、ないとは断言できない。そして、情報処理産業の秘密保護問題として最も基礎的な問題点である。なんとなれば、金融機関に対する庶民の秘密保護上の信頼も、そのベースにあるものは金融機関の企業基盤の強固さと企業自身の信用より来ているとみてよいからである。

さて、倒産・営業圧力等の情報処理産業に於いて、防止する方策は種々あると考えられるが、とくに秘密保護問題と密接する事項には次のものがあろう。

a) 企業基盤の一つとして、目標となる水準を定め、その水準以上のものを、信頼できる情報処理企業として登録・公表する。

b) 秘密保護倫理綱領を作り、これを守る社会的慣行をつくる。

c) 情報処理産業に対する不当な干渉を排除できる措置を講ずる。

等であろう。

3. 企業性格と秘密保護

情報処理産業の典型として、「サーヴィス・ビューロー」「データ・センター」即ち、わが国で言う計算センター群は、その企業性格により、秘密保護問題について若干の相違がある。

計算センターをその性格より4分類して考えてみる。

(i) 独立型(Independent)

情報処理を専業とし、かつ、親会社等の束縛をうけないもの。

(ii) 企業従属型

情報処理を専業とするが、親会社の計算室が分離独立したか、親会社が従属計算センターとして設立したもの。この場合、資本・業務量の過半数を親会社が占めるのが通常。

(iii) コンピュータ・メーカー又はディーラー従属型

コンピュータ・メーカー又はディーラーに従属する計算センターをいう。この場合、情報処理を専業とする場合もあるが、コンピュータ・セールス・バックアップ及び、ショー・ルーム的性格が強く打出される場合が多い。

(iv) 企業内計算室

情報処理を主たる事業としていないが、企業内計算室で情報処理業を行なっている場合。銀行等にその例がある。

第一の型は、情報処理専業者としての計算センターであり、一般的な秘密保護問題としての考察に従えばよい。然し、第二乃至第四の型には、それぞれの秘密保護上の固有の問題点を有している。

第一は、一定の主事業目的がある企業に完全に従属している計算センターが、その知り得たるデータ・システムを、従属企業の主たる事業目的のために使用させる可能性をもっている。例えば、銀行が一般情報処理を行なった場合、それにより蓄積されたデータは、好むと好まざるとにかかわらず、銀行の主業務である預金獲得、借付先信用調査等の情報として使用される

と考えられている事等である。

第二は、コンピュータ・メーカー又はディーラーに従属する計算センターに於いて、コンピュータ販売と云う主目的を有する以上、事業として客先のシステムを研究し、その知識の上にたって、コンピュータ・セールスを推進する事が当然であろうと考えられていることである。このような場合、秘密保護上の問題については種々、困難な問題が生じてくる。

これ等の問題は、わが国だけでなく米国に於いても同様である。この問題点について米国では、情報処理に関する委託者と、受託者間の契約上の問題であり、契約が明確であり、その罰則と両者の善意に期待する他はないとしている模様である。即ち、情報処理企業が非常に多く、又その商習慣も確立しているので、委託者は、秘密保護についても満足のいく企業をえらび、そこと確実な契約をするという自由競争と、契約概念を基礎にした考え方をもっているようである。

わが国の、この問題についてのポイントは、第一の型即ち、独立型の情報処理事業者が質的に確立していないので、委託者が選択余地が少ないことにあると考えるものもある。

4. 情報処理業上知り得たデータ利用

情報処理上知り得たデータの蓄積が行なわれ、所謂データ・バンク的な機能を果し得る情報処理業は、今後多くなると思われる。

情報処理の能率面より言えば、集中処理、データの多面利用が好ましいが、秘密問題で種々の困難が生ずる。

例えば、或る地域全般にわたり、住民の所得・地方税等を中心とした情報処理を行なったとする。（別図）これにより、勤労者の給与計算・地方税控除計算、金融機関の地方税収納代行業務、地方自治体の地方税計算・収納等の情報処理は、一つのコンピュータにより、一つのシステムで実施可能となる。この様な情報処理を行なうと、全住民の家族関係．財産関係

等のプライバシーに関係する多くのデータが蓄積する。このデータがもし秘密保護の観点なしに放置されれば、多くの恐るべき資料となり得る。

（ⅰ）管　理　面

住民管理、地域経済行政資料、治安対策

（ⅱ）信　用　面

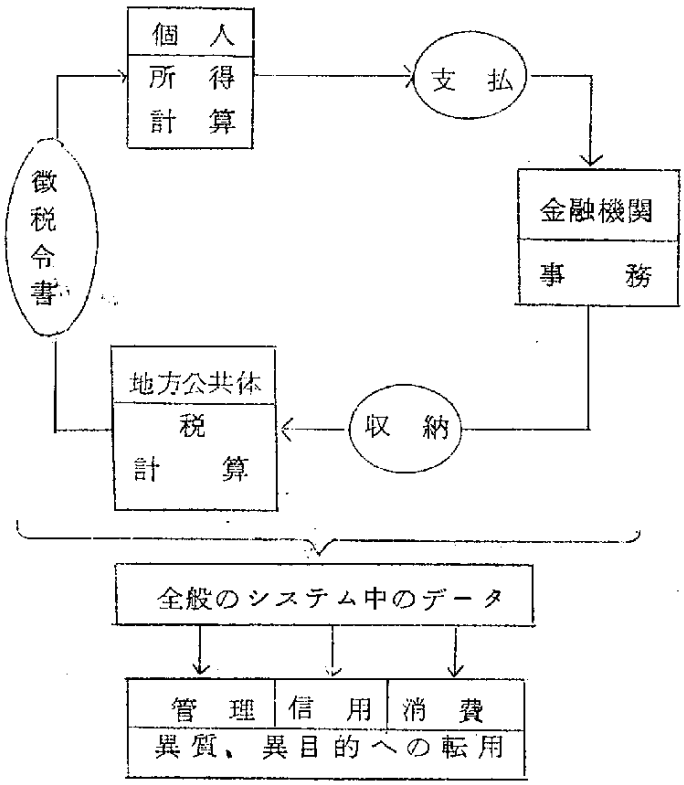
販購買、貸借、クレジット、結婚、雇傭

（ⅲ）消　費　面

セールス資料、預金獲得、等々

このように生活全般にわたる資料となる。

他で知り得たデータが悪意なことに転用されても、非常に問題が生じやすい事の一例を示したが、今後この例のように、大量の情報処理より生ずるデータの取扱いについて特別の考慮が必要な事を示している。



5. 秘密保護上の現在の手法

秘密保護上の技術上の問題は別とし、主としてバッチ処理に於ける管理上、現在わが国計算センター業界に於いて、注意されている手法を羅列することとする。

(i) 業界信用の向上

市民生活に於いて、電話、信書が他に知られるとは考えず、又、金融機関に安心して財産を信託している。

このように他業界で有している様な信用を、あらゆる面の工夫努力により情報処理業界に於いても向上させる。

(ii) 契約書の整備と実行

情報処理代行の契約に秘密保護条項を入れる。秘密に関し、なるべく具体的にその範囲、保護方法及びその洩漏に対する責任の所在、罰則等を入れる。(参考資料第3項参照のこと)

(iii) 社内就業規則の整備と実行

秘密保護条項を入れる。秘密漏洩に関する罰則は最高のものとし、解雇の場合は、業界各企業に個人名を通報する等の方法を研究中である。

(iv) 機械室管理細則の施行

機密保護上の問題点、とくに機械室への立入の許可、磁気テープ、ディスク等の保管室の立入、取扱い等を定める。プログラム・ライブラリー、種々のドキュメント、データコード等々の取扱い方法等を定める。

(v) 一業一社の受託契約

情報処理産業の営業上困難な問題であるが、一部のコンサルタント会社・計算センターも行なっていることであり、研究の必要があるとされている。少なくとも、ライバル二社の業務を同一担当者、同一事業所等で取扱わない考慮は可能である。

(vi) コードによる処理

例えば、化学製品の名称をA.B.C.、装置ディメンションをX.Y.Z.

等のかくしコードで、委託者より受託者へ情報データを投入し、情報処理業は論理展開のみ行なう。即ち、情報処理委託時に既に秘密保護をしてしまう方法をとる。

Ⅶ　プログラム上の考慮

技術問題として他の節で論ぜられるが、オペレーション可能の為のスタートのコントロールを特定オペレーションにのみ知らせるようにして、個々のシステムがみだりに処理されないようにする。

Ⅳ　技術面からみた秘密保護

つぎの5項目の過程から機密保護の技術を検討したい。

1. データ作成
2. 処理過程
3. データ管理
4. 連絡搬送
5. 管理過程

1. データ作成過程

マスター・データの作成時には、給与計算ならば個人所得や賞与、取引についてはリベート率、信用度が問題となる。トランザクション・データでは、品目別取引単価とか原価、財務内容に関する原始データが作成されなければならない。その上に、プログラマーからパンチャーやタイピストにわたるので、それだけ秘密が漏れる可能性をもつ。これを除く方法としては、バッチ単位のチェックと答案とじがある。日単位とか、１００枚単位にとじ込んで記号化されたものと、保持すべき該当欄が一致して読めないようにする。例えば、採用試験の答案は名前が採点者にはわからないようにとじている。同様に、原始帳票の設計を配慮すれば十分である。すでに、この方式でコンピュータによる採点は実施されている。

また、取引のトータルの保持ならば、新聞用紙の購入技術と同じように一個所に総てを依頼するのでなく、分散してデータを作成をすればよい。また、パーソナル・データならば、時系列的に保管されて価値あるものであるから、分散したデータ作成をプログラムで編集することになる。

一方コードの問題も重要な秘密保護策として考えられる。大蔵省ならば、ＭＯＦ、ＯＫＲとすればニューモニック・コードとして判読できるが、機密事項のプロジェクトではニューモニック・コードは使用しない。担当者

がネーミングをするが、同一のネームがないかどうかだけがチェックされる。担当者コードは、一般には、ナンバー・コードにチェック・デイジット※1を入れる。

つぎに、ディーテール・フローの記号化である。発注者と担当者間の記号化されたディーテール・フローの記号は、双方が信義のもとに保持され担当長までに継承される必要がある。これは、逆に、担当者の事故による交替ができないからである。

また、パラメータの設定では範囲を示して、実数は原数表としてデバッグ用データと一緒に渡すことによって、企業別信用限度とか、リベート査定、審査基準を保持することができる。この場合、パラメトリック・プログラム・メインテナンス技術を必要とする。

プログラムの正確性と査定の意味では、デバット用テスト・データの作り方を検討することが大切で、少ないテスト・データでは完全なデバッグをすることはできない。そして、仕様マニュアルが作成されるまでが成約準備過程である。その間は、処理方法については当時者が理解しないわけには行かないので、むしろ、プログラマー室に外部の人を入室させないこと、プログラム・デザインの試行メモは判読不能にして廃棄するようにする。

2. 処理過程

最も大きな問題は、1度プログラムが作成されマスター・データも作られ移行された場合、爾後、発生をおそれるのはこの処理過程のプロテクトとなる。

イ. ローカル・オープンの場合

計算センターに出張して処理し、時間当りのサービス料金を支払う方式であるから、むしろ社内問題となる。

ロ. リモート・オープンの場合

現状では、未だに実施されていないが今後の課題である。

ハ．クローズドの場合

計算センターに総てを任かせるので、前記に従って処理過程に入る。

これらに関し技術的に秘密を保護するためには、多くの方法が考えられているが、それ以上にまた新しい入手方法を考えていくことであろう。

A．諸技法について

イ．プログラムの作動

一般にオペレーションを開始するには、何かしらのオペレーション・キイをたたかなければならない。コンピュータがＯＮの条件を満足していても、プログラムを作動するためには、カード・フィード、コンソール・タイプインなどの後からSTART される。この過程を重視したプログラムを作る必要がある。

ロ．間接アドレス方式の作動

プログラム・ネームと処理者コードが入力されると、ロジカルにスタート・アドレスに行くようにプログラムする。これによって、ネームとコードを知っている者以外は、使用するとしても簡単にマッチされない。

ハ．コントロール番号の作成

イの方式では、ネームとコードを知られてしまえば自由に利用されることがあるが、この方式はネームとコードを入れると、新しい番号を作成するプログラムを作り、その結果に、ある記号を入力した場合のみ作動するようにするものである。

ロの方式は全部の鍵番号を知らせない方式であるが、この方式は鍵番号で全店内の番号簿を探し、それにロジックを入れてスタートさせることである。

ニ．分割方式

２つ以上のキイが組合せられたときに作動する方式である。

ホ．コントロール・ログのプロテクト

銀行のテラー・システムは、個人に権限を委譲してテラーズ・マシンで処理した。この方式は、コントロール・ログとして、一連の時系列的な操作が証拠として残されるものである。

現在のコンピュータのコントロール・ログは、自社で取りはずしや用紙をはさむことができるので、テラーズ・マシンの役割はもっていないが、簡単な改良で同様のチェックができる。

ヘ．使用者審査プログラム

リクエストが盛んになると、誰れでも使用できては賞与の評価とか、人事考課、資産内容までが管理者外に漏れることが考えられるので、ネームとコードによって使用者審査が行なわれるプログラムが必要である。

ト．リモート処理方式

応答ステーションが増加することは、それだけ一般の人々が使用する頻度が高い。電話電報のように、発信番号が逆ダイヤルから確認されるのと同様のチェック・システムとコントロール番号を併用する。

チ．コントロール番号の間違い

故意でなく、番号を間違えても作動し、ファイルが更新されてしまう。この場合は番号の作成を配慮する。

ⅰ）ルーンズ法

ⅱ）リダンダンシー法

ⅲ）7余り法

ⅳ）オッド・イーブン法

ⅴ）ＣＩＮ法

ⅵ）オート・コレクション法

などが、適用される。

（注　上記ⅰ～ⅵの詳細については付属資料Ⅰを参考のこと。）

B．フォール・バック・システムの確立

バッチ処理とリアルタイム処理のプログラムの難易度が１０倍になる

のは、同一処理内容であっても、フォール・バック・システムをもたなければならないからである。

したがって、前記のチェック事項に加味して、リクエスト頻度分析ルーティンや非関連部門からのリクエストには、対話方式のプログラムにする必要がある。そして、照会監査の時間を最少にしたフォール・バック・システムを確立する。

3. データ管理

莫大なデータが保管されるようになると、テープ、ディスク、カードなどのデータ管理を確立しなければならない。しかも、これら互換性ある媒体はそのまま使用できるので、盗難、災害の両面から問題になる。

4. 連絡・搬送

計算センターでのサービス事故には、データを授受する際の未確認によるものが多い。このチェックがなされなければ、やはり、秘密が保護されているとはいえない。

電送過程においても、ターミナルにおける数量チェックができるシステムが必要である。

5. 監査過程

社内のデータ処理内容を監査するのと同時に、外部の監査ができればよい。

アメリカではAudi-tape をはじめ、いろいろな監査用プログラムが開発されている。ロッキード社ではＥＤＰ監査基準が設けられている。また、アメリカの内国才入局では監査追跡としてのAudit-Trail を強調している。これらを勘案した技術を活用すべきである。この他、データ処理保険も検討されている。

これらを総括的に考えれば、当面の秘密保護に対する不安はほとんど解消されると技術的には考えられるものの、それによって高価な処理にはならないように配慮する技術もまた必要である。

すでに監査関係では相当細部にわたって研究されているので、参照されたいと思う。

V　管理面からみた秘密保護

情報産業の育成のためにはユーザーの秘密保護を情報産業の管理面からも早急に整備する必要がある。

問題点の主なるものとして

1. ユーザーとの契約の条項

　イ．見積り過程

　ロ．成約準備

　ハ．情報処理企業の社内的規範

2. 社内の人事管理

3. 保管方式

等があげられるが、より基本的問題としては、管理者が急速に発達したコンピューター・システムの影響力や危険の所在につき正しい知識と問題意識を持つことが要請されよう。

1. 契約と社内規範

米国の計算センターの責任者はいずれも秘密保護に関するユーザーとの間の契約の締結を重視し強調する。

COMPUTER UNIVERSITY Co.の責任者によれば「秘密の保護については契約がある。それ以上のなにものでもない」ことが強調され、UNITED CENTERS 社長も、社会秩序の基本的要素の一つは契約であり、データ・センターは顧客との間に具体的条項を締結すべきこと、これには顧客のデータを処分することに関する条項やプログラムおよび明細書の所有権に関する条項等が含まれねばならないとしている。

さて、我国で公法的に秘密保護を規制される職業は医療関係官吏、国家公務員、地方公務員、弁護士、公認会計士、税理士等であり、医師、公証人、薬剤師、薬種商、産婆等にも規制および罰則が適用されている。また、公衆通信についても秘密保護の義務規程があることは周知のところである。

ただし、公的規制のうちには実効を伴なわないものも多く、むしろ銀行、報道機関等における伝統的な半ば私的な社会規範の方が広く社会の信用を得ていることも我国の場合は常識となっている。

情報産業の性格にも鑑み、その育成促進のためにこんご公法的規制が必要となることも予想されるが、当面はユーザーとの間の私的契約および情報産業の社内規範、同業者団体の自主的規制を整備促進することが望まれる。

我国の計算センターの場合、契約書に業務上の秘密厳守や契約違反により損害を与えた場合の賠償の責任などは明記したものが多いようであり、業界の特殊事情やこんごの発展をふまえた、より具体的な契約内容を検討する必要があろう。

イ．見積過程

情報産業は、一般には、ライバル2社を同時に受注することは殆どない。しかし、コンピュータ・ディーラーは、企業形態別営業をとっている。

A社に対してサーベイを行ない、B社にもそれに近いシステムを提供することが前提で、販売促進されているとすれば、これから、どんな目的で、コンピュータを使用するかの見積り過程で、すでに、狙いは、漏れてしまう。

にも拘らず、オーダーにしなければならないときは、一流企業のように、すべて、内部の人々が見積ることになる。

同様に、処理サービスに、仕事を出すときは、適用業務に対する分析精度が問題である。

したがって、見積過程では、概念とデータ量だけの説明になる。

ロ．成約準備

概要見積りから、成約されると、深くシステム目的を知らなければな

らない。

一般には、プロジェクト名と、ソフトウェア会社の担当者名は、記号化されたものが使用されて、しかも、持続してはならない。

ハ．社内規範

一方、社内規範については下記のように可成り厳格な規程を設けている企業が多い。秘密の保護は私企業の自衛のために死活的な問題であり、これをルーズにするならば信用の失墜、注文の激減、採算の悪化を招来する。官公庁に限らず、私企業においても責任の帰趨や採算の問題が極めて真剣に考えられていることは当然のことであろう。秘密保護の見地から情報産業が官公営でなければならないとする説があるが、これは全く当らないというべきである。

秘密の定義、秘密事項

秘密の区分（極秘、秘、社外秘等）

秘密保護義務（就業規則による）

秘密事項の指定、登録番号、表示、記載、変更、取扱者を指名する役職名

社外へ委託する場合の秘密保護

複製するときの承認

秘密文書の送達方法（携行、書留等の具体的区分）

2. 人事管理面からの秘密保護

契約、社内規範更には私企業の責任意識といっても究極的には人にたいする信頼の問題に帰する。従って秘密保護重視のためには格段の人事管理に対する配慮が要求されよう。

第一は職務分権規程である。我国の現状では情報産業は未熟であり分権規程を厳格に適用することは、とくに中小計算センターの場合は実情に沿わないであろうし、斯業育成の大局展望にも副わないかも知れない。しか

し、今後進む可き方向としてオペレーター、プログラマー、ライブラリアン等の分権体制の確立が必要であろう。米国においても本来管理者たるべき者よりもプログラマーやアナリストやオペレーターが実情では多大の権限を持っていることが悩みの種のようである。

プログラムに変換可能なキーを設定し、キーを知っているオペレーターのみがプログラムをランできるようにしなければならない。米国の内部監査のチェック・ポイントによるとプログラマーのオペレーション室への出入迄チェック事項とされている。

また、ライブラリアンにはプログラムやデータファイルの使用許可権限が与えられるべきであり、ライブラリアンは作業終了時にアウトプットを管理し、その出入を記録する要がある。

つぎに広義の労務管理の問題がある。これは情報産業の問題というよりはコンピュータ関係全般の問題でもあるが、コンピュータの２４時間フル稼働が必要とされ、これに伴い可成り苛酷なオペレーターやプログラムテストの勤務条件が要請され、過保護を指摘されるパンチャーの場合においてすら、一部において意外にきびしい労働条件が散見される事実を看過してはなるまい。したがって秘密を扱う者は非組合員とするといったような配慮が民間官公庁の別なく必要であろう。

第三にセンター来客者に対する管理の問題がある。現状は内部の者はおろか、外来者にたいしてすら、カード、テープ、プログラム関係ドキュメント等が無防備のまま放置されている処が可成り見受けられる。オンラインやタイムシェアリング時代の端末機の操作等に関する高度の技術的秘密保護の問題もさることながら、より基本的な管理体制の整備が急務であることが米国における場合と同様に痛感される。

3. 秘密保護と保管方式

秘密保護の具体的方法としては保管の問題が特に重視されるが、保管の対象、場所、期限、責任者、損害防止を目的とする遠隔地での二重ファイ

ル、文書の破棄等が挙げられる。これらの大綱は社内規範にも明示されねばならない。

コンピュータ以前の時期に銀行、会社、官庁等で文書、帳票類が厳重保管されてきたと全く同じ理由で、否、データーの大量処理時代に相応しい一層厳重な方法で、カード、テープ、ディスク、プログラム関係ドキュメント等のファイルが保護されねばならないにも拘らず、ＥＤＰ部門の発達が急であり、会計制度のコンピュータ化等との均衡ある発展が見られなかったため、コンピュータ以前の基本的な保管慣行すら遵守されていない事例が少くないのである。

米国において不良ＥＤＰ要員が磁石を用いてファイルやプログラムをメチャメチャにした事例が伝えられているが正に以て他山の石とすべきであろう。

さて、保管の場所は重要度に応じ、倉庫、書庫、キャビネットに施錠保管されるべきであり、前述の如き出入の記録、重要度に応じた責任者の指定が必要であり、火災、地震等の不慮の災害に対する措置として遠隔地間に二重保管する配慮も必要である。

秘密文書の複製や破棄は依頼者の了解を得て行なわるべきであり、破棄の方法としてシュレッダーによる等が明記されるべきであろう。

以上、要するに秘密保護については情報産業の秩序づけと発展のために、競争原理を阻害せぬ範囲内において、ユーザー保護の見地に立って急速に整備されることが期待されている。

Ⅵ. 必要な対策

(1) 問題点の整理

これまでの検討により、情報産業における秘密保護という問題は大きく二つに分けて考えることができる。即ち

① 情報の漏洩の防止

② プライバシーの保護

の二つである。

前者は、情報処理サービス業或は情報提供サービス業において取扱われる情報が、それを要求する権利をもつ者以外に洩れることを防ぐ必要があるということであり、後者は、個人或は個々の企業の情報を大量に集め、それを迅速に検索することができるようになった場合にそれが濫用もしくは誤用され、個人、企業の自由が不当に奪われたり、政府など特定の機関が強大な権力を握るような結果をもたらすような事態を防ぐ必要があるということである。

①はこれからの情報ネットワークの形成と情報産業の育成振興に密接な関係のある課題である。

②はコンピュータの発達とともに発生してきた問題であるが、これは情報産業の育成、振興の見地というよりも、情報化社会において企業や、個人の権利の侵害をどう防ぐかという問題である。情報産業政策という面からいえば、情報産業の発達によって社会に及ぼすすべての影響を吟味し、弊害を少なくすることを考えなければならないのであるが、②の問題は民法、刑法、憲法など巾広い法制的検討を要するものであるので、本中間報告においては、とりあえず直接情報産業の育成振興につながりのある情報の漏洩の防止について対策を検討することとする。

(2) 情報処理の形式と秘密保護の必要性との関係

「情報の漏洩」が話題にのぼるようになった動機としては情報処理が、官庁内或は企業内にとどまらず、これらを結ぶ情報ネットワークの形成が

論じられるようになった点がある。勿論このネットワークという語は、通信回線を用いたオンライン・ネットワークに限ったことではない。オンラインであってもオフラインであっても情報が多量に蓄積され、それが企業間で盛んに流通するようになれば、情報が不当に漏洩することが問題になることには変わりはない。コンピュータをオンライン利用する場合に端末からの操作によって他人のデータが自由にとり出し得る危険は、情報の漏洩を問題にする一つの例であるが、同じ性質の危険は、計算センター施設のオープン使用の場合にもあり、これについてはハードウエア、ソフトウエアの両面における技術上の工夫が要求される。

これらの「ファイルへの自由なアクセス」を防ぐ工夫は、昔からコンピュータに採用されている計算ミスを防ぐさまざまなチエック方式と同様に、これからのコンピュータにとって必須のものと言える。

しかし、一方これらの技術的措置をとったとしてもそれだけで秘密の保護が、万全であるとは言えない。即ち、情報産業に携わる事業者の管理面の問題がある。結局情報産業における秘密保護はそれに携わる事業者の信用確立の問題につながるのであり、管理面の改善、強化により容易に情報が外部に洩れないようにすることは、ハードウェア、ソフトウェアの面で秘密保護の技術的措置を講ずるのと同じ性質の努力であると言える。したがって、情報産業における秘密保護という問題はオンライン方式とかオフライン方式とかいう処理形式に固有のものではなく、他人の情報を取り扱う情報産業に共通の問題として検討する必要がある。

(3) 法的規制の是非

多量の情報を取り扱うのはコンピュータオリエントな情報産業に限ったことではない。古くからある興信所や、私的調査会社においても同様な問題はあるので、コンピュータを利用して情報の処理、提供を行なう者のみを対象にして許・認可のごとき強い規制を加えることは適当でない。たとえ法律に根拠を求めるとしても、コンピュータを利用することによって、大

量の情報を蓄積検索する情報産業の特性を考慮しつつ、秘密保護の慣習が急速に育ってゆくよう誘導的な措置がとられることが望ましい。

(4) 望まれる対策

以上のような観点から、情報産業の育成振興のためにとるべき措置としてつぎのようなものが考えられる。

① 秘密保護の規範の提示

- ハードウェア、ソフトウェアにおける秘密保護方式
- モデル契約条項(含 損害補償方式)
- 情報保管方式、人事管理方式、内部監査方式等
- 倫理コード、モデル社内規程
- 秘密保護思想の啓蒙教育

② 情報処理技術者認定制度の活用

- 上級技術者に秘密保護の技術手法、管理手法の知識を要求

③ 情報産業を営む事業の登録制度

- 一定要件を具えた企業に特定表示の許可
- クレームの受付、監査
- 一定要件を欠くに至った表示許可の取消し
- 表示の有無に拘わらず営業は自由

付　属　資　料

Ⅰ　技術面における秘密保護の手法

Ⅱ　海外における論説

I 技術面における秘密保護の手法

1. フォール・バック・システムについて

一般には、誤りを発見したり、改訂するために、ユニット診断プログラム（Unit Diagnostics ）が用いられていた。

しかし、オンライン時代には、リアル・タイムに稼働している過程で、そのチェックをし、しかも、発見したからといって、コンピュータを、ストップさせることは、絶えずデータ入力段階でのストップが、余儀なくされるので、フォール・バック・システムがとられる。

もちろん、細部のデータについて、デバッグ過程で、起り得る条件のすべてをテストすることはできないので、オペレーション過程では、プログラム作成中には、わかっていない問題が残る。

そのたびごとに、ストップさせないために作成されたフォール・バック・システムの思想は、秘密保護のテクニックと類似しているものである。

すべてに、一律のウエイトで、秘密保護用のプログラムを作れば、リアルタイムの効果は、半減し、リモート処理のよさも、失われてしまう。

2. オペレーションの保護

自己検査番号（Self—cheaking Numbers ）を用いて、当人であることを、確認できるようにするもので、最も重要なKey である。

しかも、本人が、誤って、入力しても、保護されるので、最も一般的である。

この自己検査番号は、チェック・ディジットとか、チェック・レター、オート・コレクション・コードなど、各種の方式がある。

I ） ルーンズ法

この方法は、奇数桁を2倍にして、各桁を加算し、下1桁の10の補数をとる。

1	2	3	4	5	6
×		×		×	
2		2		2	
‖	‖	‖	‖	‖	
2	＋2＋	6	＋4＋	10	＝24

ＯＣＲのデータを確認したり、コード番号に、付加して用いられている。

Ⅱ）　リダンダンシー法

ＮＣＲのチェック・デイジット・ベリファイヤーにつけられている。

1　2　3　4　5　5
×　×　×　×　×　＝
6　5　4　3　2
‖　‖　‖　‖　‖
6 +10 +12+12+10 ＝50 ÷ 11 ＝ 4 余り 6
11−6=5
＝

各桁に異ったウエイトを乗じ、１１をコンスタントにして、除した整数余りを減ずる方式である。

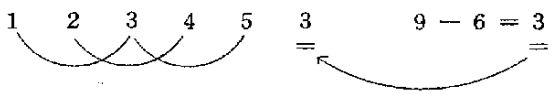
Ⅲ）　７余り法

７という数字は、０～９までに分布する性質をもっており、その整数

0 7、1 4、2 1、2 8、3 5、4 2、4 9、5 6、6 3、7 0

余りを利用することによって、チェックデイジットとして、使用できる。

Ⅳ）　オッド・イーブン法



奇数桁と、偶数桁の和を、それぞれ比較して、差を求めるものである。

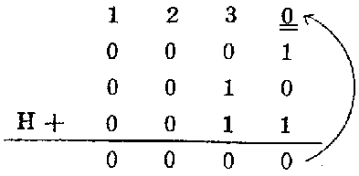
Ⅴ）　ＣＩＮ法

フランスで１０年前から使用されているもので、最も複雑なロジックをもち、デイジットでは、誤りの１０回に１回は、通過する可能性があるのに対し、アルファベットを使用するので、精度が高い。

この考え方を普遍して、最終桁のチェックを、カナ文字、英字、数字が、含められれば、さらに、改ザンできないものになるであろう。

Ⅵ）　オート・コレクション法

この方法は、情報理論を除いて、４桁の中、１桁が不明の場合には、理論的に回復できるようにするものである。



以上のコード化された記号の他、ラテン方格によるチェックもある。これらの検定できるキイによって、操作されるが、もし、理論に合わない数値が、発生しても、機械は停止しない。

優先ルーチンに割り込みを起させる信号にするのである。そしてそのデータは、フォール・バック・システムプログラムに移行する。割り込みレベルが1つの場合には、次のようになる。

(1) 以後の割り込みは、優先ルーチンが完了するまで、できない（Hardware または Software）

(2) 割り込まれたときの位置を記憶して優先ルーチンが完了するとその時点に戻る（Hardware）

(3) レジスターやラッチの内容は、保存して、回復される（Hardware または Software）

(4) 割り込みの原因と、チャンネルを確認する。（Hardware）または Software）

(5) 連続して処理するかどうかをチェックする（Software）

(6) 優先ルーチンの後で、制御は、もとのプログラムに復旧させる。（Hardware 又は Software）

データをチェックしたら、論理にかなわないときは、プログラムに誤りがあるか、機械に故障を生じたのか、データの誤りかはわからない。その場合のプログラムとしては、次のようになる。

(1) データをもう1度読ませる。

(2) プログラムを再スタートする

(3) バイオレーション・プログラムに移す。

(4) 切換えを始動する。

(5) 入力を停止する。

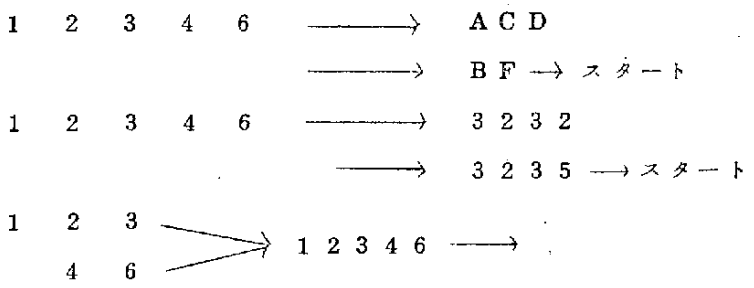
(6) 機械をストップする。

この他、試験出力によって、処置される。イギリスの銀行では、犯罪防止手段として、フォール・バック・システムを採用している。

まづ上記の番号を、そのままプログラム・スタート・コードにすれば、盗用される恐れがあるが、任意の数字を投入しても、マシンは、応答しないことになる。

次に、この番号を入力すると暗号が戻るようにして、ある条件を加味して、再入力するとスタートするシステムもある。

この場合



3. Audit Trial

この監査追跡制度は、米国ＩＲＳが「監査追跡は元帳から、１つの取引（処（処置）記録をたどって、ソース・ドキュメントに、逆に到達できる可能性を、消してはならない」として１９６４年に通達している。

この考え方は、監査を通じて、ＥＤＰの不正をつきとめるために作られたものである。大部分のＥＤＰ化は、殆んど、手作業と併行して、処理されていたため、さ程問題にはならなかったが、最近のアクセス・メモリの大容量化、低廉化によって、問題が生じてきた。

アメリカの証券会社経理主任は、ＥＤＰを利用して、６１.００万円をも着服したし、日本の某メーカーでは、プログラム・ミスを発見しないまま、加工費が、3.０００万円脱税に結びついてしまった。

秘密保護と悪用は裏腹であり、監査制度の中に、アウトプット記録と規制が重要になる。

伝票会計が、１連番号を必要とするようにトランズアクションからのファイルには、シークエンス番号を付加し、後日の挿入とか、取り出し照合は、時系列として記録され、ウォッチドッグ・タイマーによって、監査で

きるようにする。

オペレーションはコントロール・ログを、データは磁気テープでシニクエンス・ファイルが、過程ごとに記録されなければならない。

4つの監査アプローチ

① Program Control Technique

これは、途中で、故意にプログラム変更が行われたかどうかを比較するものである。

② Simulated Problem Programs

テスト・デックを用意して、時々、レギュラーのオペレーティング・プログラムを使って、正しさをチェックする。

③ 立会検査

実際の処理を、抜き打ち的に立ち会って監査するものである。

④ Audi-tape

監査プログラムの作成によって、チェックされる。

4. 勧告に対する技術的解決案

a） 政府や行政官庁は、誤った個人情報の記憶に対して、防護措置が、確実に行なえるような政策を、目的とすべきである。

Ⅰ） データバンクの機能と秘密保護

1） はじめて情報が記録されたときは必ずプリントする。

2） 変化に応じて、定期的にプリントする。

3） プリントアウト時点の授受

Ⅱ） プリントアウトの制約条件

1） 使用目的の明示

2） 前回のプリントアウト以後の使用者名

Ⅲ） データ・バンクの内容を、変更したり、消去する権限を、裁判所がもつ。

b） データ・バンクは、個人データ記録のすべてに適用される。

c） 地方公共団体、教育関係にも適用される。

d） 民間のデータ・バンクも同様である。

e） 秘密情報は、本人のものについては、公開される。

f ） 間違った記録の訂正要求が受け入れられない場合でも、真実を認めないこととは、別問題として扱う。

g ） 示された目的以外に、故意に権限外の者が、使用することは、違法である。

h ） プライバシーの不法侵害をさけるため役人は、業務に必要なもの以外は使用できないことと、陳腐化したデータを消去すべきこと。

などが挙げられている。

この問題について、考えるならば、ナンバー・システム、リクウェストに対する時系列保管、記憶保護、故障、故意の事故に対するフォール・バック・システムで、ほぼ、達成されることになる。

ただし、システムの最終責任者が、背任した場合には、この限りではない。

この場合は、Duplex Key Number にして１人では、稼働できないことにする。この他、万一にそなえては、保険をかけることになる。保険料は、月間受注額１８００万円までは、３６０００円につき、５０円である。したがって、0.１４％～0.６％で、料率の幅がある。

☆ リクエストが異常に、多く発生することはそこに、何か、特定の意味をもつと仮定すれば、度数表示にしたがって、警告システムをとることができる。

そして、バイオレーション・プログラムに移行させることができる。

Ⅱ　海外における論説

1.　英国法制研究委員会専門部会報告書

このレポートについて

保守党弁護士協会の法制研究委員会専門部会は、１９６７年７月６日、王室顧問弁護士イアン・バーシバル国会議員の提唱によって設けられた。検討を依頼されたことは、個人の自由に影響を与えるコンピュータと法律の間を研究し報告することであった。この問題は大法官庁弁護士会、慣習法弁護士会、税務弁護士会、法律事務所、国会議員、法律学会員、その他民間会社の顧問弁護士会などのメンバーから注目を浴びた。

オブザーバーとして出席されたエキスパートたちの計り知れない援助と、ＰＷＥティラー氏、ブライアン・ガルピン氏、ジェームズ・ミッチェル氏の詳細な予備調査、ならびに秘書をつとめてくれたフィリップ・タール氏のテキパキした事務処理に対し深く感謝したい。

このレポートが討議の素材となり、建設的な改革に役立たせられることを期待するものである。

アラン・キャンベル
アラン・ウッズ　} 合同議長

専門委員氏名

アラン・キャンベル（王室顧問弁護士）
アラン・ウッズ
Ｃ・Ｍ・ブロムレイ
Ｆ・Ｊ・フランシス
ブライアン・ガルピン
ダーク・ヘーン
Ａ・ピックフォード
ジェイムズ・ミッチェル
ピーター・リース
ヒュー・ロッシー（国会議員）
ルイス・スターグ
Ｐ・Ｗ・Ｅ・テーラー
Ｈ・Ｖ・ソープ
フィリップ・タール
Ｌ・Ｌ・ウェア

序　文

王室顧問弁護士、国会議員　枢密顧問官

デレック・フォルター・スミス

私は保守党弁護士協会の副議長兼実行委員会議長として、このコンピュータに関するレポートを科学が生んだ新しい道具と伝統的な自由とをいかにして調和させるかという大問題に関心をもつすべての人々に推薦することを心から嬉しく思う。このレポートは、アラン・キャンベル王室顧問弁護士とアラン・ウッズ両氏が共同議長となった委員会が作成したものである。委員会メンバーは、深い知識をもって関連する諸問題を鋭く洞察した。

このレポートは、現在は多少先き走ったように見えるかも知れないが、それは非難する根拠にはならない。将来われわれが通るべき道を示し、途中でわれわれを困らしめる可能性のある落し穴を指摘することは、ある意味では保守党弁護士協会の仕事であり、また価値のあることだろう。

コンピュータの急激な進歩のテンポに合わせて、個々の市民のプライバシーを守るために必要な措置をとることは必ずしも容易ではない。そのバランスをとるために、政治家、弁護士はじめ、すべての思慮ある人々が、当面する問題と取り組んでいるのである。もっとはっきりいえば１９６８年１０月３日に上級裁判所が秘密情報を保護することに関して下した決定が問題とされる。

この委員会の成果として生まれた報告書は、保守党弁護士協会全体の意見として発表される。私は報告書をすべての思慮深い読者に提出し得ることを、この立派な成果を生み出してくれた人々のために嬉しく思うものである。

１９６８年１１月

問　題

コンピュータが発達して、わが国の住民とその活動に関する詳細な情報を集め、記憶しそれを利用することができるようになってきた。時がたつにつれてこれらのシステムは公私ともに事務処理を革命的に変革する。しかし、このような変革から生まれる効果は、プライバシーという商品が次第にへっ

て行くという犠牲の上にのみ求められるのである。さらに個人の情報システムが広く利用されるようになればなるほど、それが誤って伝えられる機会は多くなり、被害も大きくなる。またコンピュータの利用とデータバンクの創設は、万一運用を誤ると、圧政の道具となりうる大量の情報を政府に提供することになるということも認識せねばならない。

個人のデータを記録したコンピュータ・システムがこのような圧政に利用されるのを防ぐためには、現在、あるいはここ十年の間に個人に新しい権利を与えねばならないのか、あるいはこのようなシステムに法的規制をする必要があるのかということを調査することがこのレポートの目的である。とくにこのシステムを利用する効果とプライバシーが調和できるのか、どこでどの程度までお互いに犠牲を強いることができるのだろうか。保守党の弁護士として、われわれはプライバシーの一面だけを示すにすぎない自由という問題に重点をおいて出発した。しかしわれわれは、わが国の近代化に専心する政党に属していることを十分自覚しているし、われわれが行なった勧告に反した考え方とも適当にバランスをとりたいと考えている。

わが国で現在起りつつあり、また将来起るであろうと思われている問題の本質は、アメリカの経験に基いた3つの例にもっともよくあらわれている。

例　1

ここ10年以内に、大部分の商人や月賦販売業者あるいは顧客の信用状態をすぐ知りたい人たちは、コンピュータによって信用を調査する協会に頼らざるを得なくなるだろう。その協会には莫大な数の個人情報をもったデータバンクがある。情報は協会のサービスを利用する人に提供される。情報をコンピュータ処理することによって、協会は個人の信用状態を即座に知らせることを目的としている。商人の運搬車が品物を誤配したら、商人の請求書に合った品物は配達されない。顧客は代金を支払うのを断わる。一年間代金を支払わないと、本人の知らぬ間にそれが商人の勘定を決済するコンピュータによって信用調査協会のデータバンクに自動的に入れられる。あとになって商人は品物が顧客に届けられなかったことと、勘定が訂正されたことを知らされる。しかし顧客が長期間代金を支払わなかった記録は、協会のデータバ

ンクから消えないのである。それからのちは、顧客は協会のデータバンクの情報が間違っていることを知らずにいる中に、他の商人から信用買いや月賦販売を断わられ、家や土地の賃貸を申し込んでも拒否され、破産者と同様に扱われる。さらに法律上の権利を与えられない限り、自分の名誉を損なう記録があるということを発見することは決してないだろうし、記録が間違っていることを知らされない限り、誤った評価に対して協会から法的に賠償をうけることはないだろう。

例　2

こんご１０年の間に、事業主に幹部社員の信頼度や忠実さを知らせ、幹部社員たるべき人の資格や能力に関する情報を提供する機関ができて、幹部社員や将来幹部たるべき人に関するあらゆる種類の断片的知識をつめこんだデータバンクを使うだろう。データバンクにはそれらの人の交友関係、恋愛関係、財産、身分、経歴がいろいろ入れられる。その機関はコンピュータシステム、を利用してあらゆる個人情報をたやすく手に入れるようになるだろう。しかしプライバシーの侵害はないだろうか。ごく一部であっても間違った情報、歪められた情報、マトをはずれた情報があったならば、それによって起る被害を考慮しなければならない。すべての社員がどこか新しい出発をするチャンスを待ちのぞんでいるのだろうか。若いときの無分別な行為の記録が一生の重荷となることはないだろうか。

例　3

政府や地方公共団体のための国家的なデータバンクが作られた場合のことを考えてみたまえ。税務署、保健所、国家保険庁その他の政府機関が受け取ったあらゆる情報が、この唯一のデータバンクに入れられた場合のことを考えてみたまえ。由々しい結果が起り得るのだ。税金納入の不正は減るだろうしかし適切な規制がなければ、データバンクは役人なら誰にでも知人の財政状態や病気その他の個人的な事柄について完全な情報を与える。医者は患者の財政状態をすべて知ることができるし、税務署に勤めている隣人は、何の関係もないのにわが家の病人について、本人以上に病気や手術の状況を知ることができるのである。

総括的に言うと、個人情報のデータバンクをもつコンピュータシステムを利用することによって起り得る危険性の主なるものはつぎのような項目に分けられる。

(a) 誤った情報のインプット、記憶、流通

(I) 事実が不完全で誤解を招く

(II) そのような事実や誤った判断に基いて、必要な条件をつけずに分割したり統合したりすることによって、全部又は一部を使って誤った意見を述べたり推測したり分類したりする。

(b) コンピュータシステムを所有している人およびその従業員による情報の不正使用、例えば権限外の人にたいして情報を流すこと

(c) 部外者が故意又は過失で情報を引き出したり使ったりすること

(d) プライバシーの侵害、即ち他人の情報を集め、照合し、伝え、使用すること、あるいはごく少数の人だけに知らされるべき情報が広く流布されたり使われること。

コンピュータ　メーカーとユーザー

コンピュータメーカーとユーザーは、これら一般的な危険性について注意されているし、この危険をさける2つの主な手段―技術上と管理上の一を講じて来た。技術的な手段には、インプットのチェック、エラーの防止と修正策、データ移動の制限、パッチ・リーダー、キー（Key）、バー（Bar）、パスワード、スクランブラー（Scrambler)などがある。管理上の手段には、インプット、記憶、プログラム、アウトプットの内容に関連する処理、技術訓練、操作方法の改良、技術的コントロールの選択と管理、プログラマ、システムアナリスト、システムエンジニア、オペレータなどスタッフの選択と管理、ファイルをチェックするための忠告と助言などがあげられる。

大部分のコンピュータメーカーは、これらの事柄に関するわかり易い訓練法、指導法を用意している。標準ができつつある。

しかしこれらのコントロールや標準で全部をカバーすることは不可能である。例えば何千という出所から出てくるデータの正当性と妥当性をチェックするコンピュータ所有者の能力は制限される必要があるだろう。ここから法

律が検討される。

現　行　法

コンピュータを利用する以前にも、記録を編集するときにある程度同じような危険性はあったのである。わが国では１０８６年ウィリアム一世が作った最初の土地台帳の編集の時からこの問題は発している。その時以来、多くの技術上の進歩が個人のプライバシーを脅かして来たし、事実侵害してもきた。そして問題は発展して来たのである。印刷、望遠鏡、カメラ、タイプライタ、ミニ・マイクロフォンの発明は「個人」の事情に立入ってせんさくし、記録し、それを広める力を増してきた。しかしコンピュータシステムの出現は、問題のスケールを急激に変えた。以前にはまだ我慢できる程度だった被害が、急激に増大するようになったのである。以前の小規模な問題であった場合には現行法でもそれに対抗する武器があった。上記(a)から(d)までに述べたことをまとめてみるのもよいことだろう。

(a)　誤った情報のインプット、記憶、流通

とくにコンピュータ利用以前の記録にこの危険があった。裁判所のファイルに間違った記録が入ると、公営住宅の賃貸借ができなくなった。興信所のファイルに間違った記録が入ると月賦で品物を買うことができなくなった。たとえ本人が記録の誤りを知ったとしても、被害者がそれを訂正させたり消し去らせる法的な対策はなかった。しかし誤った記録が入ったり、それに伴って誤った推測が流れたりすると、名誉毀損の法令が適用された。この法令が守られることは、誤った記録がファイルやコンピュータから除かれるのと同じ効果がある。しかし名誉毀損を犯人とした人の権利をきびしく拘束することには限定的だが特権の学説がある。この学説は情報を作り、それを受けとることによって利益を受ける一つまり個人情報のデータバンクが最もよく利用される分野でとられている。この学説がとられると、犯意が証明されなければ名誉を損なうような誤りを口にしても被害は償われない。例えば、情報が本当だと信じて、間違ったことを言った結果名誉を傷つけた場合、本人に悪意がなく、個人的利益を得る動機から行動したのではないときには、法的責任はないということになっている。従って一般

的なルールとして、信用調査協会は、無意識の誤りや、会員に提供した信用を損なう情報に対して、おそらく名誉毀損の責任はないことになろう。しかし、もしデーターバンクを持っている民間会社が料金をとって信用調査情報を提供した場合なら、名誉毀損の訴えを起し得るだろう。

最近の状況から予想すると、長期的には情報をデータバンクに入れるときおよびシステムを操作するときに十分注意が至らなかったために損害をうけた人に対して、その被害の訴訟を起す手続きを裁判所が確立するだろう。しかし現状では、法律が情報を集められている個人を十分保護するどころの段階ではないのである。

名誉毀損の被害者が損害賠償の訴訟に勝つと、本人の希望によっては裁判所にコンピュータシステムのオペレータに対して、二度と間違った情報を流さぬよう禁止令を出させることもできる。この命令を破るとそのオペレータを侮辱罪で懲役に服させることができる。

しかし賠償をとるには実際上いろいろな困難がある。被害者は記録が誤っている証拠を見つけることはできないだろう。たとえ証拠を見つけたとしても、その記録が公表されたことを証明しなければならない。もし彼が間違った記録があることを発見しても、オペレータがそれを訂正し消し去ることを断われば誤ったままで発表されるおそれがあるという理由で禁止命令をとりつけることができるだろうか。記録の誤りが単純で、発表されると取りかえしのつかぬ被害をうけるところではその禁止命令が認められてもよい。しかし申し立ての記録が本当に間違ったものかどうかという問題が残っており、それが決定しない間は、名誉毀損の訴訟をする前に中間的なあるいは一時的な禁止命令は認められない。

(b) コンピュータシステム関係者による情報の不正使用

現行法はこの危険性に対処するには割合よくできている。コンピュータシステムから情報をこっそり引き出すことは、ファイルから引き出すよりむずかしい。コンピュータシステムに記憶されている情報を要員が不正使用すれば、現行法にふれることになる。データ処理サービスに関する郵便局法は１９６７年、データ処理によって局員が得た情報は、職務上又は法律によって要求されるものを除いて、処理要員の同意なしに発表できない

ことにした。１９６４年に定められた所得税法は、税申告に含まれる情報について、署員の職責または法の定めるもの以外は発表しないことにしている。１９１１年の機密保護法もやはり、厳重な予防措置を講じている。

同様に民間のコンピュータシステム所有者やオペレータが情報を不正に使用すると、顧客やユーザー、情報提供者との契約条項に違反することになり、損害賠償を要求されることになるだろう。銀行員が預金者の秘密を守る義務があることは、すでによく知られているが、預金者の勘定が銀行のセントラルコンピュータに保管されていても同様である。システムの顧客は、システムの所有者やオペレータが顧客に関する秘密情報を権限もないのに発表したり、ゆすったりしないように、裁判所に命令を出してもらうことができる。しかし秘密情報でも、公益のためあるいは警察に犯罪を通報する場合には何の保護も与えられないだろう。コンピュータシステムの所有者やオペレータだけでなく、たまたま秘密情報を知り得た人全部にも裁判所の命令が認められる。秘密情報の発表を制限する裁判所の権限は、直接システムの顧客でなくとも、契約上何の関係がなくとも、情報に関係する人に及ぶのである。それはプライバシーの全面保護にまで波及し、(d)に述べるようにさらに細部にわたるのである。

(c) 部外者が故意でなく情報を流したり、誤って引き出したり、使用した場合

権限のない部外者が情報を引き出したり、使ったりするのを防ぐには、法律上の対策よりも物理的に引き出したり使用したりできないようにすることの方が大事である。権限外の者がコンピュータシステムに接触したり、それを機械的に妨害することは、システム所有者から損害賠償を訴えられる侵害行為になる。しかし電気的に盗聴することが可能であれば、それは決して侵害行為にはならないだろう。システムの利用を許されているユーザーが、誤って他人の情報を引き出したり使ったりしても、契約上あるいは規定上の条件に反したことになる。ユーザーの情報を盗みとることが可能になるような不注意な管理やオペレートの責任に対して、同じ条件が、ある場合には所有者を保護することになり、ある場合には保護しないことになる。ユーザーは当然、秘密情報を故意又は偶然に引き出したり流したり

した者に対し禁止命令を出せる権利がある。

(d) プライバシーの侵害

すでに述べて来たように、現行法では、たとえどんなに秘密なものでも不正確な情報でも、その情報を集めたり照合したりするのを禁止するルールがない。しかしある場合には秘密やプライバシーを守るために、記録されている情報の使用をコントロールされる。たとえ秘密を守る契約上の義務がなくとも、裁判所は禁止命令を出すことによって秘密の漏洩を防ぐことができる。高等法院長スインフェン・イーディ氏は1913年に関連した法律をつぎのようにまとめている。

「大法官庁が長年とってきた原則は、不正な手段で得られた秘密情報や、洩らしてはならない情報が流されるのを防ぐことである。禁止命令は、秘密情報が流されるのを防ぐとともにそれが複写されるのを防ぐ。万一コピーがとれていたら、それ以上にそれが複写されたり、広められたりするのを防ぐ」

しかしこの救済手段も、秘密情報を扱うと認められた人にのみ裁判所が適用して来たにすぎなかった。

さらに、公益に役立つ場合は他に発表してもよいという情報が、処置を誤って発表された場合には裁判権は及ばなかった。このため警察に犯罪を通報する場合は、秘密を守ることについて例外が認められた。洗濯屋が新聞に、洗濯代の値上げは選択雇傭税（Selective Employment Tax）の負担によるものだと虚偽の広告をした場合、その新聞に洗濯屋の利益に関する情報を流すことは許されると広く信じられている。現状では例外の範囲は広いし、漠然としている。このほかにも例外はあるだろう。どんな場合にも秘密情報とは何かということは、裁判所で確定されていないのである。秘密情報がある官公庁に与えられたとき、それを他の官公庁に知らせるのを制限する管轄権はない。裁判所が現行法のもとで、発表を禁ずる法律上又は契約上の条項がないのに、問題となっている特殊なケースの発表を妨げるかどうかは明らかでない。

現行法の欠陥

上述の同じ見出しで考えてみるのが便利だろう。

(a) 間違った情報のインプット、記憶、流通

現在は上記の問題に対する法的措置は、誤った情報が公けにされた場合にのみ起る。しかも限定された原則できびしく制限されている。誤った情報が記録されており、それが流されたということを発見する適切な方法はない。だから現行法ではコンピュータ・データバンクのオペレーションでも、実質的には何の予防策もないといっても過言ではない。

(b) コンピュータシステムの関係者による情報の不正使用

(c) 部外者が、故意又は偶然に情報を引き出したり使用した場合

そのような不正使用、それに伴なう故意の引き出しは、現行の私的賠償から、刑事裁判所で処罰する罪にすべきである。

(d) プライバシーの侵害

プライバシーは、わが国では常に基本的人権に関するものとされてきた。その侵害を正当化するのは、公共政策に重大な影響のあるときだけに限られていた。一例として、信書の秘密ならびに電話の傍受制限があげられる。これらを許すのは内務大臣の権限だけであった。個人情報データバンクが設立され使用された結果、プライバシーが侵害されるのは2つの形がある。第1は今まで考えられていたよりもはるかに大きなスケールで個人情報が集められ記憶されること、第2は今まで考えられていたより遙かに広い範囲に個人情報が流れることである。法律が個人情報の収集や流通を制限すべきか、もし制限するならどの程度までかについては容易に答えることはできない。一方では知識の大規模な蓄積による効率化と、他方では他人の詳細な情報を自由に使うべきでないという個人の権利をバランスさせる必要がある。会社に関していえば、商売上の秘密を守る権利が考えられる。明らかにコンピュータシステムを情報の収集、照合のためだけに使うことには何の異議もない。また何の不都合もなく、情報を受けとっている人に情報を流すことにも何ら問題はない。だから顧客の勘定明細を記録し、その本人にだけ提供するようにプログラムされた銀行コンピュータシステムや、マネジャー、支店の顧客担当者は全く問題がない。しかし、もし税務署が、システムに記憶された情報を自動的に流用することは全く問題が別になる。

税務署は官公庁が持っている全国的データバンクに入っている情報を全

部流用できるだろうか。税収のごまかしを困難にするという点に限って言えば、その方法を許すことにも理由がある。しかしこの場合、「重要な犯罪」と「つまらない犯罪」との区別をつけねばならない。電話の盗聴にも同様の区別があるように。だから全国データバンクは、そこに入っている情報を無差別に役人に流すことを防ぐ規定を作っておかねばならない。

民間データバンクに関するプライバシー侵害の点では、現行法はアイマイであり不完全なものである。もし重大なプライバシー侵害が起ったときには、不当な侵害を抑える民法上、刑法上の限定された条文を設けるよう現行法を改正すべきである。

結　論

われわれはつぎのことを勧告する。

(a) 政府や行政官庁は、誤った個人情報の記憶に対して、つぎのような防護措置が確実に講ぜられることを政策の目的とするべきである。個人情報データバンクは、いろいろな目的に適した人を選び出すために設けられるのだから、情報が間違っていたら目的を失なうし、損失を与えることになるのだから。

(I) つぎの場合には、データバンクが機能を発揮しうるために秘密にしておかねばならぬ情報は別にして、情報をプリントアウトして顧客に提供しなければならない。

(1) はじめて情報が記録されたとき（あるいは一定期間内に）

(2) 前回プリントアウトされてから、何の変化もないときを除いて、適当な間隔で定期的に

(3) プリントアウトの費用を請求し、支払った都度

(II) プリントアウトされたものには、つぎのことが述べてなければならない。

(1) 記録されている情報を使う目的、あるいは前回プリントアウトして以来何に使ったか

(2) 前回のプリントアウト以後、記録してある情報を使った者の全員の氏名と住所

(Ⅲ) データバンクのオペレータに不平を持つ人の出願について、裁判所は、上記(1)に関する秘密情報は別として、データバンクに入っている情報を変更したり消し去ることを命令する権限を持つべきである。

(Ⅳ) 裁判所は、これまでに間違った情報をうけとって満足できない人は、変更し又は消し去った情報を知らされるべきであり、その場合の費用はデータバンクのオペレータが負担すべきだと命令する権限をもつべきである。

(Ⅴ) データバンクに入れてある情報は、前回顧客に提供されたプリントアウトに述べられた目的以外には使われるべきでない。

(b) この法律条項は、個人データ記録を入れてある政府のデータバンク全部に適用されるべきである。例えば現在別々の政府機関で別個に保管されているデータ記録を統合するために設けられるデータバンクにも適用されるべきである。しかし警察や機密情報機関の記録は例外として完全に秘密を守られる。

(c) 同様な法的規制は、地方公共団体が、教育施設の校舎や土地を割当てたり、スタッフを選んだり昇進させたりするのに使うデータバンクにも適用されるべきである。

(d) 同じ効力をもった法律条項は、民間データバンクにも、つぎの場合適用されるべきである。ある分野のデータバンクが、その分野の情報をほぼ完全に支配する地位を占めている場合、例えば家具の月賦、特定産業あるいは特定業種への雇傭など。データバンクの所有者が顧客との間で、この法律条項に反する契約を結んでも無効である。誤ったプリントアウトを提供したり、情報を違った目的で使ったり、使うのを許すことは、刑事訴訟法によって罰せられる犯罪である。

(e) プリンアウトから除外される秘密情報として扱われるものは、ケースによって限定されることが必要である。秘密情報として通常どんなものがあげられるかについては、かなり制限された見解がとられるべきである。例えば、部下の昇進が適当か否かを決定する目的で作られる「秘密報告」は、本人に見せるべきだし、本人はそれに挑戦する機会を持つべきだということは公平な考えである。現実に陸軍士官の年1回の秘密レポート」ではそ

れが行なわれている。だから何かの目的で適任者を選択するレポートは、その関係者に秘密にしておくべきだという考えには言い分が沢山ある。しかしこれはコンピュータシステムに限った問題ではない。法律に規制されたデータバンクに入れられているレポートに関する政府の方針は、データバンクに入っていないレポートに関するものと殆んど変化はない。これはもっと区別して検討しなければならぬ大問題である。われわれは余りにも無関心すぎたのである。

(f) 提供されるプリントアウトに必要な法的措置には、間違って記録された情報の訂正を要求して失敗しても、真実を認めないということは別だということを明らかにしておくことが必要である。

(g) プリントアウトに特に示された目的以外に情報が使われることが違法とされるならば、権限外の人が故意に情報を流したり使ったりすることは犯罪として民法上の事件となるべきである。個人情報データバンクのオペレータとユーザーが、情報を不正使用したら民事訴訟の責を負うべきだということが、データバンクの従業員自身によって自覚さるべきである。データバンクを操作するときに重要な誤りを犯して有罪となった人は、個人情報データバンクのオペレータとして雇わないように、また関係しないように裁判所が指令することも考えられてよい。

(h) プライバシーの不法な侵害をさけるためいろいろな情報源からプールされた情報をもっている全国的データバンクや地方公共団体のデータバンクも、規制の対象となるべきである。

(I) 役人は自分の仕事を遂行するに必要なデータだけを使うことができるよう制限する。

(II) 時代おくれになって不適当になった情報を消し去ることを考える。

(i) 上記(h)に関連した規制を厳密に守ることを保証するために、(h)に該当するデータバンクは、そのデータバンクを利用する官公庁以外の独立機関あるいはそれら官公庁の幹部に全く関係のない独立委員会の監督をうけるべきである。

(j) 上記(d)にあげた民間経営のコンピュータシステムが提供したプリントアウトをみると、プライバシーの侵害が多いことがわかる。それは一般の慣

激を買うだろう。そうなれば個人の情報を集めたり、記録された情報を流すことに対して何らかの規制が必要となる。その規制は、前以て一般大衆に受け入れられそうもないものを法制化しようとするよりも、一般大衆の反応を見てから決めた方がよいだろう。

2. コンピュータとプライバシーの法律

リチャード・I・ミラー

アメリカ人は、生まれたとき両親の所得税申告書に記載されてから社会保険局の死亡年金を支払われるまで、ずっと記録を残していることは今では周知のことである。例えば銀行、信用サービス、保険調査業などが持っている民間のファイルに加えて、郡、州、連邦機関が、われわれの学業成績、財産所有権、登録一犬や事業や結婚の一、兵役簿、収入、公けの申請書、裁判記録がある。記録はファイル・カード、マイクロフィルム、パンチテープその他磁気記憶装置に入っている。そして何百という民間、政府、教育、軍隊システムの記録センターを通じて使われる。生命が芸術に先んじ、　科学がフィクションを追い越す時代には、記録センターが共通語でお互いに話し合う社会が来ることは容易に想像できる。そして個人は直観的に自分の歴史がクモの巣にからまってしまうのを感ずる。

コンピュータとプライバシーの権利との関係が深く心配される理由は、他の手段や技術とプライバシーの権利との関係と全く異質であるからである。チョッキのポケットに入るテレビカメラ、隠し撮りカメラや様々の監視装置と違って、コンピュータは「侵入」しない。見ない。血も流さないし、解剖もしない。勝手に証拠を集める手段としてさえ使うことはできない。むしろ与えられた情報を貯え、オペレータの要求に従って記憶装置の中にある他の情報と関連させ、関係をつける。全部を知っており決して忘れさせないという機械の姿は、多くの人に恐れを抱かせる。これがプライバシーの概念を検討し直さねばならぬ十分な理由なのである。

第１に、その概念に関するコンピュータのオペレーションを見てみよう。第２に、プライバシーの概念について、アメリカのケースと法律上どう考えられているかを簡単に調べ最後に法律がどんな役にたつかについて２～３の勧告をしよう。

売り物の情報

データの取得と販売は活発なビジネスである。クレジット、保険、個人調査が始められている。小売信用会社とか協同信用局などの組織は、州や連邦法規により許されている。裁判所の書記は、どんな裁判記録でもわずかな代金で証明されたコンピュータを送るだろう。大きな小売信用会社は依頼人にどんな捜査も以前の調査で作られた記録を引き出すことによって強化されるということを保証する。弁護士のサービスは、あらゆる種類の公文書を知ることによって成立する。しかし、兵役についていない人の完全な書類を編集することは時間の浪費であり金のかかることだということは真実である。従って結論から言うと、プライバシーは、データ検索が非能率であることによって辛うじて守られているのである。

今までは、データの不正使用や流通といっても、寄付金リストの賃貸しとか販売のような余り大きな被害のない程度のことであった。個人データの調査が増加し、それが価値を持つに至ったのは、巨大なコンピュータの出現が齎した変化である。代表的な信用ファイルには、住所、家族状態、勤め先の場所、給料概算、信用供与額、支払費用などが入れられており、保険会社のファイルの場合には、医療や病院の記録や「背徳」－異常な夫婦関係、同性愛、大酒のみとか、保険金額に影響する社会的観察まで入れられている。それはもはや全国民の生命に関するあらゆる文書が早く安く利用するか〝どうか〟の問題ではなくて、〝いつ〟〝誰によって〟〝どのような状況のもとで〟利用されるかの問題である。

一般の注意は、予算局の統計標準室が提案した「全国データセンター」案に集中しているが、個人データの記憶と検索に関心を持っているのは連邦政府だけではないということも明らかである。たとえ予算局の案が上下両院の委員会によって流産したとはいえ、個人データ流通の割合は急速に社会の私的な分野で広がって行く。民間の情報処理機関はさておいて、政府関係機関ばかり攻撃することが多いが、「証明」が目的でない記録を個人データセンターを利用して集めることからプライバシーを侵害する危険は、公僕も、債権者や訴訟当事者も同じである。政府機関の行き過ぎを矯める法律を作ることだけでは十分ではない。むしろプライバシーの法的概念は、個人をあら

ゆる角度からの襲撃から守っている信書の秘密と同じ考えに立たねばならない。

コンピュータのエキスパート達は、(1)統計情報システムと、(2)機密情報システムとの間に一線を画する。理論的に言えば、統計情報システムは、個人のグループ、つまり「住民」に関する特性を明らかにする情報を作る。これに対して機密情報システムは、個人データを個人として統合する。統計的な質問は、「ロスブリー地区住民の何割が年収3,000ドル以下か」というようなもの、機密情報の質問は「ジョン・ドウ氏の年収はいくらか」というようなものである。

統計情報システムは機密情報システムに使われないようにデザインし管理しなければならないという議論をする人たちがいる。それらの人たちは、秘密統計情報の発表を法律で禁じられている国勢調査局の例を指摘する。他のエキスパートたちは区別することに反対し、コンピュータのスピードが進み、コストが下って行くのだから、機密情報の目的を達成できるように統計情報システムの中にナマのデータを貯えておく方が効率がよくなると反論している。時系列の研究には同一のコードがつけられねばならない。そうすれば1968年のロスクブリー地区住民の収入は、収入傾向に関する情報を引き出すために1967年の収入と対比されるに違いない。

門外漢にとっては、分析者がナマのデータからできる限りの統計情報を引き出して満足しているように見える。統計情報システムと機密情報システムを別にすることに賛成している。しかしトランプを切る新しい方法は常にあるものだ。有能な分析者は、いつもデータの目新らしく有用な相互関係を調査している。より大きなコンピュータを使う方が分析に容易であるのは事実だから、統計システムと機密システムを完全に切りはなすのは、せいぜい一時的なことであろう。

1890年「ハーバード法律展望」にウォーレンとフランダイスが書いた有名な記事以前には、アメリカの法律には「プライバシー」について法的権利が認められてなかった。プライバシーという考え方は一例えば憲法の捜索と逮捕条項、特権を与えられている通信の慣習法、商取引の秘密の条項、名誉毀損の法律の中に含まれてはいたが、プライバシーの侵害が明らかに罪として法廷で認められることはなかった。今でも簡単に述べられる権利ではな

い。事実それは4つの別々な、むしろ関連のない法律行為として分析されてきた。

1. 一人でいたいという権利の侵害
2. 通常の礼儀を踏まずに個人的私事を公表すること
3. 文書を偽造して、ある個人の考えに反することを述べ、誤ったイメージを一般に持たせること
4. 許可なく個人人格のある要素を商売に利用すること

以上各々の形の中に、プライバシーの「権利」は、独りにしておかれる権利、せんさくされたり、のぞかれたり、嗅ぎ回ったりされない権利としてあらわれている。プライベートな人間でありたいという個人の欲求が「プライバシー」とは別の条項の中に含まれ法律問題の特徴でもある。捜索と逮捕のケースで、大審院は、プライベートな通信を不当に妨害するために使われる電子的、光学的、音響的手段を非難した。大審院はカッツ対アメリカ合衆国政府の訴訟の中で、「憲法の第4修正条項を〝プライバシーの権利〟に適用することはできない。・・・」が、プライバシーに対する人間の〝一般的〟権利を守ること―他の人から離れている権利―は、財産や生命を守るのと同じく、各州の法律の中に大きく残されている、と述べている。

コンピュータによって提起された法律問題は違う。それは、情報を不当に引き出すのではなくて、自発的に知らされた情報の正確さや不当な使用を意味するのである。大審院が上記のケースでみているように、「意識的に一般に見せているものは、自分の家庭や事務室の中のものでも、第4修正条項に守られる対象にはならない」。だから特権を与えられている通信と名誉毀損のローカル法は、プライバシーの問題にとっては少しは適切なものである。

前者の場合、法律は、夫に妻の、あるいは弁護士に依頼人の秘密の情報を無理に洩らすように強いることはできない。一組の夫婦は法律的にはお互いに秘密を知らせることを禁じてはいないけれども、少くとも自発的に知らせ合うことは、第3者の手に入るおそれのあるときは別として、原則として許されることである。名誉毀損に該当する表現とは、周囲の思慮ある、社会的地位のある階層の人々の心に憎み、あざけり、軽蔑を起させるように暴露するようなものに限定されている。

多くの場合出版物の自由に対するプライバシーの権利のバランスが問題となっている。幸いにも、法律は物理的な侵害行為を必要としない。しかしこれらのケースには原告に〝関する〟記述が原告に〝よる〟記述と別に含まれているのが特色である。法廷は許可されない伝記の出版を禁ずるであろうが、プライベートな電話の会話を発表することに対する損害賠償を課することはないだろう。だがこれはコンピュータによって侵される「プライバシー」の種類に関してあらわれて来た慣習法の範囲においてのことである。もしプライバシー保護の判例をみたいなら、イチジクの葉以上のものはまずない。

2つの関連問題

法文は同時に2つの方向に発展しつつある。われわれは政府が情報を蓄積しそれを人民から隔離して権力を持つことに関係しているし、法の力で引き出した情報や、ある特定の目的のために自発的に提供された情報を発表できないようにされている。だから情報の有効性をつよめる「情報の自由」法と、その有効性を禁ずる「プライバシー」法がある。

知る権利を増進するために、議会はすべての市民がワシントンの官庁で何が起っているかを知る権利を与える「情報の自由」法を通過させた。この法律は、理論的にはつぎのものを除き、すべての書類を公開している。

1. 国防に関する書類
2. ＦＢＩのファイル
3. 所得税申告書ファイル
4. 特許出願ファイル
5. Executive branch memoranda
6. 通商上の秘密および産業財務データ

すべての官公庁が快よく法に従う筈はない。事実ある種の記録は発表されていない。在郷軍人局の記録、商業上の産物のテスト、食料・薬品局の新薬採用、民間航空委員会の苦情書などもその中に入っている。他方農務省は普通以上に協力的で、前年の政府支払いが5,０００ドル以上の農家全員の名前を記した厚い書類を誰にでも閲覧させると発表した。当局の説明によれば、これらの記録を発表することは（理論上はいつも公開されるものだったが）

・・・「新しい法律の結果ではなくて、農務省の新しいコンピュータの結果である。コンピュータによって始めて、いままでは郡単位でしかわからなかった農家への補助金データを全国的に編集することが出来た」

コインのもう一つの面は、上記に示された判例にあてはめるべく、つぎつぎにあらわれるプライバシー法規によって示される。例えばニューヨーク州のプライバシー法規は「品物を売る広告や販売推進のために、他人の名前、肖像、写真を、同意を得ずに勝手に使うこと」を禁じている。守られる利益は、本来経済的なものだが、法務行政の面では、社会的道徳的考慮が払われる傾向にある。

権利と保護のバランス

技術的な意味でなく、広い意味で「プライバシー」に関する法規上の最も重要な発展はもちろん盗聴や拷問、公共機関の謄写版利用などによって集めた証拠の妥当性に関するものである。このような場合、プライバシーに対する個人の権利は、犯罪に対して自からを守る社会の権利と比較される。これらの議論には、話を聞いたものが自発的に内容を発表することは含んでいないし、われわれの主題に直接関係していない。しかし重要なことは、プライベートな人格に加えられるコンピュータの独特な攻撃に対して、法律は無関係だということである。

自動車のデザインの例に見るように、製造責任の分野では、法律が効果的に規制できるのは術語だけであるということが経験によって知られている。ドライバーをテストし、免許を与え、監督するだけでは不十分である。法律は車そのもののデザインにも影響しなければならない。空気や水の汚染のような健康と安全の問題とは別に、公共の利益を守る生産規制の概念は広がっている。そこで、個人データを貯え、それを配布するコンピュータの使い方について考えられるいくつかの技術的防護策を勧告しよう。

1. 個人データを伝送する通信回線に対して最低限度の暗号化措置を工夫すること。こうすれば電話の盗聴より技術的に費用がかかるので、データの盗受はしないだろう。
2. 個人データは決して"直ぐに理解できる状態"でファイルに蓄積しない

と。単純な方法で貯えることは、ある意味で、たちまち安全な貯蔵庫をカラにすることになる。

3. プログラマーが故意に、また、不注意に個人データに最短ルートのアクセスを行なうことができないプログラムが、データ・バンクに用意されているかどうかを、銀行記録の監査と同様に標準化し、監査すること。
4. 個人データの照会がどこから発せられたか、その源を検知し、記録する装置をコンピュータに内蔵させること。

これらの提案は、疑いなくコンピュータのコストをあげるだろう。丁度座席ベルトやダッシュボードが自動車のコストをあげるように。しかし、もしコンピュータが自動車と同じく、社会で重要な役割を果すように運命づけられているとするならば、今こそ付加的コストを作る時である。

プライバシーの法的定義を広げるためには間違った情報を流したり、本当の情報を悪意をもって使うことから起る最初の名誉毀損事件をまつ必要はない。エール法律学校のチャールズ・ライヒ教授は、憲法の著者はその時代に理解されたあらゆる方法でプライバシーを守った、と見ている。彼等は言論や宗教や罪になる知識を守った。彼等は権限のない捜索や逮捕に対して人民を守り、兵隊が民家に泊るのを禁じた。武器を身につけることすらプライバシーの適用と考えることができる。彼等の関心を今日の世界にあてはめるとしたら、少くもこれらの大胆な提案を検討してはいけないのだろうか。

法的権利の拡大

1. データを第3者に流す目的のために、いくつかの源泉から個人データを集める政府機関とか民間人とか工場は、つぎのことをする必要がある。
   a 人々に自分達のデータが集められているという注意を与える。
   b それらの人々によって証明の目的のためにデータが処理される。
2. 官公庁が個人のプライバシーを守るためのプログラムを発表し、最高行政官庁がこれを認めない限り、政府機関は個人のデータを貯え第3者に流す目的でデータ処理機械を買ったり使ったりする権限を与えられない。政府機関に操作と設備を自由に使わせる基準は、順次作られ採用されるだろう。
3. 個人データを集め、それを配布する仕事をしている公共機関、工場、代

理店やその従業員は、間違ったデータを流したり、本当のデータを悪意をもって流したために被害をうけた人に対して責任をとるべきである。傷つけられた人々は、そのデータの流通を禁ずる権利がある。

全体主義の社会、病院あるいは刑務所生活の観察が教えてくれることは、個人の生活は、本人が選ばない限り開いた本であるべきでないということである。社会はページが時には人目にさらされることを要求する権利がある。しかし、ページをつき合せることによって本を編集し、著者の許可なしに内容を出版することを望む人は、正確さと正しい使い方について責任をもたなければならない。ナタニエル・ホーソーンとコンラッド先験主義者たちは、19世紀に、秘められた心を調べることは最も重い罪だと考えた。もしわれわれが自からのテクノロジーに達するのを防ぎきれなかったら、もう秘められた心は存在しないだろう。

参　考　資　料

I　法律条項、社内規程、契約書

I 法律条項、社内規程、契約書

1. 秘密漏泄規程および罰則の例

（例示）

医　　師……刑法第１３４条
薬 剤 士　　〃
薬 種 商　　〃
産　　婆　　〃
弁 護 士　　〃　　及び弁護士法第２３条
公 証 人　　〃
医薬関係官吏等……医療法第７３条
国家公務員……国家公務員法第１００条
地方公務員……地方公務員法第３４条
公認会計士……公認会計士法第２７条、２９条、３１条
税 理 士……税理士法第５４条
統 計 官……統計法第１４条、第１５条、第１９条の２

〔1〕 刑　　法

第１３４条

医師、薬剤士、薬種商、産婆、弁護士、公証人又は此等の職にありし者、故なく其業務上取扱いたる事につき知り得たる人の秘密を漏泄したる時は６月以下の懲役又は１００円以下の罰金に処す。

2　宗教若くは祈祷の職に在る者又は此等の職に在りし者故なく其業務上取扱いたることにつき知り得たる人の秘密を漏泄したる時又同じ。

〔2〕 医 療 法

第７３条

当該官吏若しくは吏員又はその職にあった者が、故なく（第５条第２

項（国及び地方公共団体は病院又は診療所が不足している時は計画的に整備しなければならない）又は第２５条（市長は診療所等の管理者に対し必要な報告を求めたり当該官吏若しくは吏員に立入り検査をする事が出来る）の規定による診察録又は助産録検査に関し知得した医師、歯科医師又は助産婦の業務上の秘密又は個人の秘密を漏した時は、６月以下の懲役又は一万円以下の罰金に処す。

２２．職務上前項の秘密を知得した他の公務員又は公務員であった者が、故なくその秘密を漏したときも前項と同様である。

〔3〕 国家公務員法

第１００条

職員は職務上知る事の出来た秘密を漏らしてはならない。その職を退いた後と言えども同様とする。

② 法令による証人、鑑定人等となり、職務上の秘密に属する事項を発表するには所轄庁の長（退職者についてはその退職した官職又はこれに担当する官職の所轄庁の長）の許可を要する。

（罰　　則）

第１０９条

第１００条第１項又は第２項の規定に違反して秘密を漏した者は一年以下の懲役又は３万円以下の罰金に処する。

〔4〕 地方公務員法

第３４条

職員は職務上知り得た秘密を漏してはならない。その職を退いた後も同様とする。

② 法令による証人、鑑定人等となり、職務上の秘密に属する事項を発表する場合においては、任命権者（退職者についてはその退職した職又はこれに相当する職に係る任命権者）の許可を受けなければならない。

（違反者は一年以下の懲役又は３万円以下の罰金に処す…第６０条）

〔5〕 公認会計士法

第２７条

公認会計士又は会計士補は、正当な理由がなく、その業務上取扱ったことについて知り得た秘密を他に漏らし、又は窃用してはならない。公認会計士及び会計士補でなくなった後であっても同様とする。

第３１条

公認会計士又は会計士補がこの法律又はこの法律に基ずく命令に違反した時は大蔵大臣は第２９条各号に掲げる懲戒の処分をすることができる。

第２９条

公認会計士又は会計士補に対する懲戒処分は下の三種とする。

1. 戒　　告
2. 一年以内の業務停止
3. 登録の抹消

〔6〕 税理士法

第５４条　（税理士の使用人等の秘密を守る義務）

税理士の使用人その他の従業者は正当な理由がなくて税理士業務に関して知り得た秘密を他に漏らし又は窃用してはならない。税理士の使用人その他の従業者でなくなった後においても、また同様とする。（違反した場合は２年以下の懲役又は３万円以下の罰金に処する……６０条）

〔7〕 弁護士法

第２３条

弁護士又は弁護士であった者はその職務上知り得た秘密を保持する権利を有し義務を負う。但し法律に別段の定めある場合はこの限りでない。

〔8〕 統計法

第１４条　（秘密の保護）

指定統計調査の結果知られた人、法人又はその他の団体の秘密に属す

る事項については、その秘密は、保護されなければならない。

第１５条

何人も、指定統計を作成するために集められた調査票を、統計上の目的以外に使用してはならない。

② 前項の規定は、行政管理庁長官の承認を得て使用の目的を公示したものについては、これを適用しない。

第１９条の２（罰則）

統計官、統計主事その他指定統計調査に関する事務に従事する者、統計調査員又はこれらの職にあった者が、その職務執行に関して知り得た人、法人又はその他の団体の秘密に属する事項を、他に漏し、又は窃用したときは、これを１年以下の懲役又は５千円以下の罰金に処する。

② 前項に掲げる者が、行政管理庁長官の承認を得た場合の外集計された結果を第７条（指定統計調査の承認及び実施）の規定により定められた公表期日以前に、他に漏し、又は窃用したときは、これを５千円以下の罰金に処する。

③ 職務上前２項の事項を知り得た第１項に掲げる者以外の公務員又は公務員であった者が、同項の行為をしたときもまた同項の例による。

2. 社内規程の例

(1) 機密保持規程－㈱コンピュータアプリケーションズ

（目　　的）

第 1 条　この規程は、機密保持に関する事項を定めたものである。

（機密の定義）

第 2 条　機密とは、部外へ公表または洩らすことをゆるさない業務上の秘密をいう。

（機密事項）

第 3 条　機密事項とは、次の社内外に関する事項で、機密として指定されたものをいう。

1. 経営政策
2. 技術計画、研究開発事項、技術基準
3. 技術輸出入、技術提携に関するノウ・ハウ
4. 営業計画
5. 予算・決算、原価・価格
6. 受注その他社外との契約およびこれに関連する事項
7. 顧客より機密事項として指定されたものおよび業務上知り得た資料・情報
8. 前各号のほか、外部の察知により会社が不利となる事項

（機密事項の区分）

第 4 条　機密事項は次の通り区分する。

1. 極　秘　　最も秘密を要する事項で、社内外を問わず特定の関係者以外へ公表をゆるさないもの
2. 秘　　前号につぐ機密事項で、担当部課（またはこれに準ずるもの）および特定の関係者以外への公表をゆるさないもの

3. 社外秘　　社外への公表をゆるさないもの

（機密保持義務）

第 5 条　社員は、社員就業規則に基づき、この規定を遵守し、業務上知り得た機密を関係者以外に洩らしてはならない。

（機密事項の指定その他）

第 6 条　(1)機密事項の指定、区分、変更ならびに関係者および保持取扱者の指名は、担当取締役以上において、これを行なう。ただし、担当取締役以上において適当と認める場合は、部課長（またはこれに準ずるもの）に行なわせることができる。

(2)第 3 条第 7 号において顧客より機密事項として指定された場合、担当取締役以上は、直ちに機密として指定し、適切な措置をとるものとする。

（機密事項の表示）

第 7 条　機密文書およびこれに準ずるものには、区分、登録番号その他管理上の必要事項を表示するものとする。

（機　密　簿）

第 8 条　機密事項の作成、指定、区分、変更、解除、破棄、配布その他管理上の必要事項は、機密簿に登録記載の上、これを行なわなければならない。

（保持取扱者）

第 9 条　機密事項の保管、配布、受入その他管理上の事務は、保持取扱者がこれを行なう。

（保管容器）

第１０条　(1)機密事項は金庫または鉄製の鍵のかかる容器の中に保管するものとする。ただし、機密事項の内容によってやむを得ない場合は、機密

保持上最も適当と認める方法によることができる。

(2)金庫およびこれに準ずるダイヤル式の番号は保持取扱者以外に知らせてはならない。

(3)鍵を使用する容器の場合、その鍵は、保持取扱者以外のものが保管してはならない。

（機密事項の破棄）

第１１条　(1)機密事項が不用になった場合は、焼却、細断その他の方法により破棄することができる。

(2)機密文書の調整、複写などに使用した原稿、謄写用紙、タイプ原紙、複写紙、フィルムなどは、用済後焼却、細断その他の方法により完全に破棄しなければならない。

（制限区域）

第１２条　機密保持上、必要と認める場合は、関係者以外の立入制限区域を設けることができる。

（社外に対する機密保持の措置）

第１３条　(1)機密事項の研究、開発、計画、立案、作成その他を社外へ委託する場合、または顧客その他に機密事項に関する資料を提示もしくは貸与する場合は、機密保持に関する契約書またはこれに準ずる文書を取りかわさなければならない。

(2)前項の資料は必らず回収しなければならない。

（対外発表）

第１４条　機密事項の対外発表は、担当取締役以上においてこれを行なうものとする。ただし、担当取締役以上において適当と認める場合は、部課長（またはこれに準ずるもの）に行なわせることができる。

本規程は昭和４１年１０月１日から実施する。

(2) 秘密保全規程－コンピューターシステム㈱

（目　　的）

第 1 条　この規程はコンピュータシステム株式会社の業務運営上必要な他社及び他の機関（以下他社と称する。）の秘密の保全に関する事項を定める。

（定　　義）

第 2 条　この規定における秘密とは、他社に関する知識及びそれに関する文書、図面等（以下「秘密文書等」と称する）をいう。

（適用範囲）

第 3 条　この規定に従う義務のあるものは、コンピューターシステム株式会社の社員、見習及び臨時に使用せるものである。（以下社員という）

（関係職員）

第 4 条

(1) 管理責任者

他社の秘密事項全般を総括するもので原則として常務取締役がこれにあたる。また必要に応じて副管理、責任者を任命する事ができる。副管理責任者は管理責任者を補佐し又は代行する。

(2) 取　扱　者

管理責任者の指定する職員で秘密事項に関する取扱いをする職員。

(3) 保　管　者

管理責任者の指定する職員で秘密文書等の保管を担当する職員

（秘密を守る義務）

第 5 条　第 3 条に該当するものは、他社に関する秘密を関係職員以外の者に漏らしてはならない。また秘密の保持には最善の注意を払わねばなら

。

（関係職員の指定及び連絡）

第 6 条　管理責任者は他社の秘密文書等の受理後、直ちに関係職員を指定し、その名簿を他社に提出しなければならない。

（受渡記録）

第 7 条　保管者は秘密文書等について第6条により区分の指定及び変更、解除があったとき及び他社との受渡があったときは、文書規定により定める簿冊に直ちに記録しなければならない。

（立入禁止）

第 8 条　管理責任者は社内施設で、秘密事項が取扱われるため保全上必要あるときは、その場所に立入を禁止、または制限することができる。

（複　　製）

第 9 条　秘密文書等を複製するときは、管理責任者が他社の承認を得なければならない。

（印刷等の実施）

第１０条　秘密文書等の印刷、複写等をする場合は秘密保持上支障のない場所で関係職員または管理責任者の指定した社員が実施しなければならない。この際、原紙、不良品は第１８条に準じ完全に処分しなければならない。

（外部への伝達及び送達）

第１１条　社外の者に秘密事項を伝達または送達するときは他社の許可を受けなければならない。

（送達方法）

第１２条

(1)　秘密文書等を送達するときは関係職員または管理責任者の指定する

社員が携行するものとする。

ただし、管理責任者の許可したもの、もしくは他社の承認を得て書留便等の確実な方法で送達することができる。

(2) 送達については授受を明確にするために、受領証または授受簿により受領印を徴するものとする。

（保　　管）

第１３条　秘密文書等は保管者が保管するものとし、容器は金庫または文字盤鍵のロッカーに保管しなければならない。

また、保管容器の備え付けある部屋の入口は施錠可能なものでなければならない。

（貸出し）

第１４条　秘密文書等の貸出しは管理責任者が前もって他社の承認を得なければならない。

（検　　査）

第１５条　管理責任者は秘密の保全状況について年２回以上の定期検査を実施するものとする。

（事故に対する処置）

第１６条　秘密文書等の紛失漏えいがあったとき、またはその疑いがある場合は直ちに管理責任者に報告し適切な措置をしなければならない。又管理責任者は直ちに他社に連絡し、措置を仰ぐとともに、その対策には積極的に協力するものとする。

（罰　　則）

第１７条　本規定に違反ある場合には、就業規則第６２条の適用を受ける。

（反古に対する処置）

第１８条　秘密事項に関連する反古、計算途中結果等は、所定の屑箱に収納し毎日一回定時に関係職員の立合いのもとにシュレーダーで裁断するものとする。

（その他）

第１９条　前各条に該当しない特別の事項の追加及び規定の改廃、変更は取締役の承認を得なければならない。

本規定は昭和４３年６月１日より施行する。

3. 契約書の例

(1) 事務代行契約書

事務委託人株式会社○○銀行（以下甲という）と、事務受託人株式会社××計算センター（以下乙という）との間に事務代行に関し、下記の通り契約を締結する。

第 1 条　甲は甲の△△計算事務とこれが付帯統計事務の代行を乙に委託し乙はこれを受諾した。

事務代行の方法は別に定める。

第 2 条　甲乙何れかが契約を解除せんとする場合は、相手方に対して3ケ月前に書面により申出るものとする。

甲乙何れかが料金および代行事務内容を変更せんとする場合は、事前に相手方に申込み、協議するものとする。

第 3 条　乙は事務代行にともなう業務上の秘密を厳守するとともに○○原簿その他の別に定める関係書類の保管の責任を負うものとする。

第 4 条　甲乙何れかがこの契約に違反し、そのため相手方に損害をあたえた場合はそれぞれ損害賠償の責任を負うものとする。

第 5 条　この契約に定めてない事項が発生した場合は、甲乙協議の上紳士的に解決するものとする。

上記契約履行の証として本証2通を作成し、甲乙署名捺印の上各1通宛所持するものとする。

(2) 契　約　書

△△△△△作業の一部委託について○○局（以下甲という。）と株式会社××計算センター（以下乙という。）との間で下記のとおり契約を締結するものとする。

記

（作業代行）

第1条　甲は△△△△△金納入通知書および別紙各種統計表の作成作業を乙に委託するものとする。

（期　間）

第2条　乙の作業代行期間は、昭和40年4月1日から始まり解約の申込みがあった月から6カ月後（解約申込みの月は含まない）の月末に終了するものとする。

（解約および契約の一部変更）

第3条　甲、乙何れかが契約を解除せんとするときは、前条にもとずきあらかじめ相手方へ書面にてその旨を申出るものとする。

甲、乙何れかが契約内容の一部変更を行なわんとするときは、2カ月前に相手方へ申込みあらためて双方で協議するものとする。

（手　数　料）

第4条　作業代行（諸用紙一切を含む）の1カ月委託手数料は○万件までは最低金額、金○○万円也と定め、○万件を超過する○万件に達するまでは1件毎に○円として甲は乙へ支払うものとする。

（支払条件）

第5条　前条の手数料は毎月末日締切、翌月20日まで現金にて甲が乙へ支払うものとする。

（秘密保持）

第 6 条　乙は甲に関する業務上の秘密保持を厳守するものとする。

秘密とするデータの範囲は別に定める。

乙は秘密保持上のデータおよび計算室管理規程を定め、甲の承認をうけるものとする。

（納　　期）

第 7 条　甲は乙が作業代行のため必要な △ △ △ を整理の上、乙へ提出するものとする。

乙は上記 △ △ △ 及び料金納入通知書、統計表の一部を甲へ 2 日後に納入するものとする。

（契約違反）

第 8 条　甲、乙何れかがこの契約に違反して相手方に損害をあたえたときは、それによって被る損害は損害を与えたものがこれを弁済するものとする。

（契約外事項）

第 9 条　この契約に定めていない事項が発生したときは、甲、乙協議により誠意をもってこれを解決するものとする。