43—R 003

情報産業における秘密保護

調 査 報 告 書

昭和44年6月

財団法人　日本情報処理開発センター

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」に関する調査報告書である。

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、ソフトウエ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。

このほか、ソフトウエアの作成、受託を業とするもの、あるいはコンサルタントなども次第に増加しております。それらの人々も職業上、他社の秘密に深くタッチする機会が多いだけに秘密保護の対象となると思いますが、このたびは、情報処理サービスおよび情報提供サービスを中心としたインプット、アウトプットを主な対象とすることに限定しております。

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日本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、ここに結論をまとめ、報告書を作成いたしました。なお、付属資料「技術面における秘密保護のための要素」および「技術面における秘密保護の手法」は、日本ＥＤＰ株式会社が担当しました。

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。

委員諸氏のご努力に心から感謝の意を表します。

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

（敬称略・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
	鈴木秀郎	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	(財)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

海　外　文　献

参　考　資　料

1. 情報産業における秘密保護の必要性

1.1 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ものと考えられ、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、宗教家を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。

1.2 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。

1.3　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。

1.4 本書の主な内容

本報告書では、これらの問題に対処するための方策について、広い観点からとりあげる。

まず、第2章では、海外における秘密保護の状況について、とくに米国および英国の文献からその実情を紹介し、将来わが国の情報産業の発展を考慮する上での示唆を与える。

第3章では、わが国における秘密保護の現状と問題点について、計算センターを中心に考察し、将来発展が予想されるデータバンクにおけるデータ利用、および秘密保護上とられている現在の手法を紹介する。

第4章では、情報産業の進展とプライバシーについて、データ・バンク等に個人情報が集中管理されることを予想して、プライバシーの法的根拠および判例の法的解釈のあり方、さらに個人の情報機関設立の動き、各機関における秘密保護対策の現状について紹介する。

第5章では、技術面からみた秘密保護対策について、中央処理および端末装置に関する技術的手法を体系的に整理し、解説を行なう。

第6章では、管理面からみた秘密保護対策について、契約上の問題、人事管理上の対策、およびデータ・ファイル等の保管方法について論じ、管理上規範となるべき方法を分類・整理し、実務の参考に資する。

第7章では、以上を総合して、秘密保護における必要な対策について、法的規制の是非および望まれる対策を総合的に体系化し、それらの特長について解説を加えると共に、将来の指針を与える。

付属資料として、日本ＥＤＰ株式会社による、秘密保護に関する技術報告書を収録するとともに　海外文献として、外国における関係論文を翻訳

し参考に供する。また参考資料として、秘密保護に関する法律条項および社内規程・契約書（例）を呈示する。

2. 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。

2.1 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、他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、民間企業情報処理企業、情報提供業と、広範な利用形態が考えられる。

表2－1　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

2.2 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保護は、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。

2.3 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。

2.4 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。

2.5 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。各種の公的・私的機関は、われわれが生まれた瞬間から、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・記録を行なっている。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。

(イ) 現在、計画・開発中の秘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。

(ロ) 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。

(ハ) 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。

3. 国内における秘密保護の現状と問題点

3.1 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、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、文章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。

3.2 企業基盤・信用と秘密保護

情報処理産業が、秘密の保護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。

(1) 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、心配は杞憂にすぎないかもしれない。

(2) 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。

(3) 税務署、警察署、労働基準監督署等官公庁の調査

米国において、計算センターは、「税務署を拒否する」との慣習が出来つつあるときいている。

これは、データの集積が生じている情報処理産業は、依頼人の種々の秘密を保護するため特別な犯罪的行為等を除き、官公庁およびこれに類似した機関のデータ調査に応ずるべきでないという意味である。わが国においては、このような問題が生じて、依頼人の利益を害したという実例はないが、そのような危険がないとはいえない。従って、法的整備式は秘密保護慣習をつくるように努めることが好ましい。

以上の3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。

(1) 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

(2) 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

(3) 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。

3.3 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。

(1) 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。

(2) 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。

(3) コンピュータ・メーカー又はディラー従属型

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。

(4) 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である。

3.4 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（図3－1）。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。

(1) 管　理　面

住民管理、地域経済行政資料、治安対策

(2) 信　　用　　面

販購買、貸借、クレジット、結婚、雇傭

(3) 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。

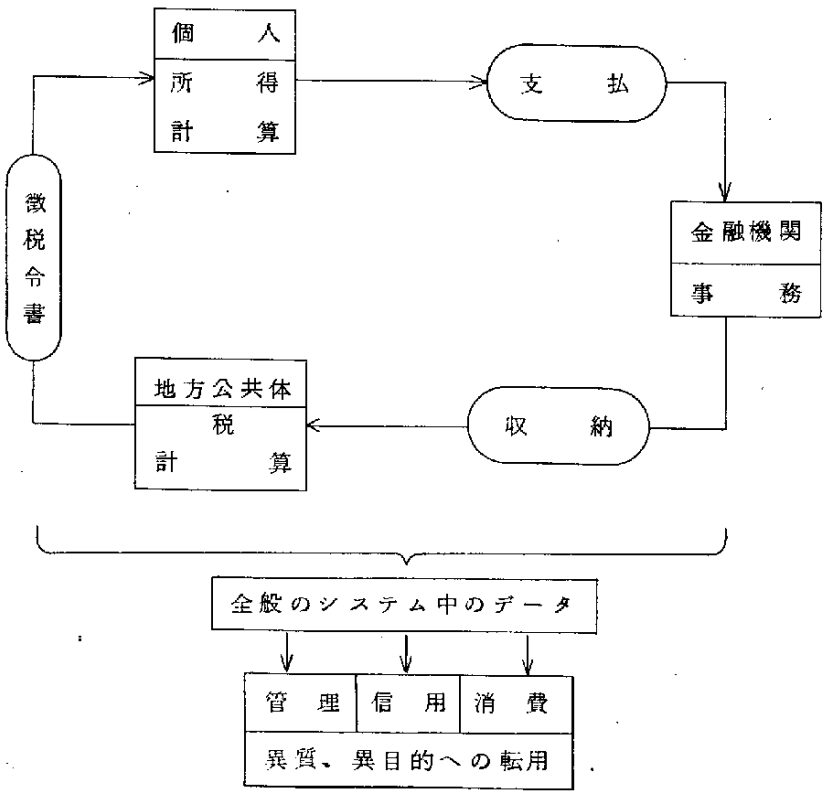


図 3 － 1　住民の所得・地方税等の情報処理

3.5 遠隔情報処理における秘密保護の実情

現在、わが国で通信線を利用した遠隔情報処理を行なっているのは、法的制約もあり、一企業内、あるいは、特定企業集団内の、メッセージ・スイッチング、座席予約システム、バンキング・システム等を主としたものであり、不特定多数に対する情報処理は行なわれていない。

従って、一般的な遠隔情報処理に関する秘密保護上の問題がすべて提起されているという状態には到っていないのが実情である。しかしながら、近い将来、通信回線が公開されることを前提として、研究が進められている。

遠隔情報処理の問題は、中央処理装置・端末装置および通信回線の三区分におけるそれぞれの問題と、全システム上の問題とを加え四つの問題点がある。

中央処理装置および端末装置それぞれにおける秘密保護の問題は、バッチ処理における問題点とほぼ類似している。

通信回線の問題点は、一般電信電話と同様、誤交換・盗聴等々の問題の他に、データ伝送上のエラー等固有の技術問題がある。

遠隔情報処理における秘密保護上最も検討を要する問題は、局地的な処置にとどまらずシステム全体の問題として考える必要がある。

本問題の多くは、技術面にあり、別の章に詳述されているが、現在わが国で行なわれている最大公約数的な手法に次のようなものがある。

(1) 端末機の利用は、一以上の鍵等により定められたオペレータ以外の操作を不能にしている。

(2) 端末側としては、中央処理装置の呼出し、および特定データの検索等には、2つ以上のキー・コードの組み合わせの合致により始めて可能とし、事故防止に努めている。

(3) 中央処理装置は、端末よりの呼出しに対し、コール・バック方式およびその他のチェック・システムを加えて、端末の確認を行なった後、データ処理に応ずる。

又、それらはターミナルに記録する。

3.6 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。

(1) 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。

(2) 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）

(3) 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。

(4) 機械室管理細則の施行

秘密保護上の問題点、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。

(5) 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。

(6) 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。

(7) 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タ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。

(8) 遠隔情報処理上の特別な考慮

遠隔情報処理は、一般バッチ処理と種々ことなる秘密保護上の問題がある。現在は、前節で述べたような手法が主として用いられ、又、更に後章で述べられる技術上の手法で秘密保護を行なうことができる。

4. 情報産業の進展とプライバシー

コンピュータの利用と秘密保護の問題が取り上げられるとき、海外においては、まず「プライバシーの侵害」が重点として論議されていることは、第2章に述べられているとおりである。しかしわが国においては、企業の秘密が情報処理企業から漏洩するのを防ぐことだけに重点がおかれ、プライバシーの侵害については殆んど論議の対象とはならないし、また十分検討されようとする機運も動いていないのが現状である。

しかしながら、わが国でも、ようやく最近信用取引、クレジット販売の流行とともに、個人信用の調査が必要とされ、調査会社の設立が実現される動きが活発化するに至って、プライバシー侵害の危険も全くないとは必ずしも言えない状勢となって来た。こんご情報産業が急速に発展していくに従って、いかなる問題が予想されるか、それに対してどのような対策が必要となるであろうかを考えておくことは、重要なことであろう。

4.1 プライバシーの権利の根拠と責任

プライバシーとは「私生活を公表されない」権利ということができる（日本弁護士連合会コンピュータ研究特別委員会副委員長宮原守男氏）が、その法的根拠は憲法第13条「すべて国民は、個人として尊重される。生命、自由及び幸福追求に対する国民の権利については、公共の福祉に反しない限り、立法その他の国政の上で、最大の尊重を必要とする」に求めることができる。そしてそれが侵害された場合は、民法上、刑法上の責任が追求される。

（注）軽犯罪法1条23項〔違反行為〕

左の各号の一に該当する者は、これを拘留又は科料に処する。

23　正当な理由がなくて人の住居、浴場、更衣場、便所その他人が通常衣服をつけないでいるような場所をひそかにのぞき見た者

民法235条1項〔観望施設の制限〕

疆界線ヨリ1メートル未満ノ距離ニ於テ他人ノ宅地ヲ観望スベ

キ窓又ハ縁側ヲ設クル者ハ目隠ヲ附スルコトヲ要ス

刑法１３３条〔信書開披〕

故ナク封緘シタル信書ヲ開披シタル者ハ１年以下ノ懲役又ハ二百円以下ノ罰金ニ処ス

法制上の責任という場合には、民事上の責任（損害賠償責任）と刑法上の責任（刑法で罰せられる）があるが、現行法では、公務員・医師等、職種によって秘密保護の義務をもつもの（本報告書参考資料参照）以外は、民事上の責任を負うだけである。この点については、法律改正案が審議されている（宮原氏）が、同じ損害賠償についても、法律用語では、①契約を結んでいるのにそれに違反した場合を「債務不履行」といい、②契約関係がないときには「不法行為」という。

また、わが国では「プライバシーの侵害」は、「名誉毀損」と同意語として使われている傾向があるが、この両者には、つぎのような差がある。（宮原氏）

(1) 名誉毀損は、「個人の社会的評価を低下させる」ことに対するもので、公表された内容が「真実でないとき」に責任を負うものである。

これに対し、プライバシーは、「本人の感情を保護する」もので、公表された内容が「真実であるとき」でも、責任を負うことになる。

従って、ここで注意しなければならないことは、技術面、管理面での秘密保護対策がどんなに完全に行なわれても、個人情報のファイルの作り方や、情報作成の方法如何によっては、プライバシーの侵害は起り得るということである。すなわち、技術面、管理面で秘密の漏洩や、誤った情報の流通を防ぐことはできても、プライバシーの侵害を防止することは、性質が違う面があるということを十分考えねばならない点である。

(2) 名誉毀損は、民事・刑事両方の責任があるが、プライバシー侵害は、まず民事で扱って、その範囲を越えるときにのみ刑事問題とされる。

（補完の原則）

4.2 わが国におけるプライバシーの判例と考え方

わが国のプライバシー問題で、最も注目を浴びた判例は、「宴のあと」

事件（原告・元外相有田八郎、被告・作家三島由紀夫ほか、昭和３９年９月２８日東京地裁）であるが、ここで関心があることは判決そのものよりも、プライバシーの保護に関して、法的な解釈を明確に示していることである。

ここでは、どんな場合にプライバシーの侵害になるかの要件として、つぎの３点をあげている。

(1) 私生活の事実あるいは事実らしく受けとられる恐れのあるもの。

(2) 一般人の感受性を基準として、本人の立場に立ったら公開を欲しないもの。

(3) 一般人にまだ知られていないもの。

このほか「芸術的価値のあるものおよび有名人、公的存在の場合にはプライバシーの保護にも制限がある」など、その後のプライバシー問題の判決に影響を与えるような解釈を与えたが、情報産業の場合でも、これがそのまま適用される。

将来、情報産業が発展して行くとともに、個人情報を入れたデータ・バンクが当然出現するであろうし、それを利用する場合に、

(1) データが誤っていて、その情報がそのまま公表されたとき

(2) データ・バンク側の誤った操作によって情報が誤ってアウトプットされた場合

(3) 誤った情報が訂正され、ファイルが更新される間の時間的ズレによって誤った情報がそのまま公表されたとき

(4) たとえ事実であっても、以前の過失がいつまでも記録されていて、現在は全く関係がないにも拘わらず、それが訂正されず不利益を蒙むったとき（これは警察の犯罪記録あるいは公安関係の調査に例がみられる）

(5) その他、故意に誤った情報が公表されたとき

など、さまざまな問題が予想される。

しかしながら、現実には証拠の立証が極めて困難であるために、プライバシーの保護はむずかしい。日本弁護士連合会ではコンピュータ研究特別委員会を設け、目下法律の改正を検討中である。

4.3 個人に関する情報機関設立の動きと現状

現在わが国で個人の情報を扱っている機関としては、（コンピュータを利用しているといないとを問わず）、月賦販売が流行するにつれて、月賦の支払いを確保し、貸倒れを防止するために顧客の信用情報を集めることを中心に発展してきた。東京の中野区役所のように、住民のあらゆる記録をコンピュータ化しているところも出現しているが、これらの機関が、どのような秘密保護措置をとっているか、現状をみるとつぎのとおりである。

(1) 中野区役所

住民の収入、家族状況その他あらゆる個人情報がコンピュータに集中記憶されているが、個人の秘密保護のうえには特別な措置は講じていない。というのは、地方公務員については秘密保護について、いろいろな法規で規制されている（参考資料参照）ので、これを遵守している限り問題はないし、現実に何の問題も起こっていない。

ときに外部の計算センターを利用する場合もあるが、その場合はマシンを借りるだけで、操作はすべて区役所の職員が行なう。アウトプット資料は全部持ち帰って、情報が第三者に流れるのを防止しているし、月賦業者、百貨店などから個人情報の提供を求められることは多いが、一切応じていない。

(2) 日本割賦協会

協会内に信用登録機関として信用情報交換所を設け、信用調査の合理化、貸倒れ、行方不明者の調査を行なっているが、現在はまだコンピュータ化はしていない。

しかしながら、秘密保護については相当慎重で、つぎのような措置をとっている。

(イ) 会員から提供された顧客の支払事故記録（遅延又は不払い）は、正確かどうか顧客本人に直接問い合わせを行ない確認しているので、情報が誤って記録されることはない。

(ロ) 顧客の信用情報は、会員にだけ通報する。（会員は理事会の承認を得なければ入会できず、月賦業者以外のものの入会をチェックしている）

(ハ) 顧客の信用情報は、問い合わせをうけた会員にだけ行ない、顧客記録の公開は一切行なわない。不払い者の氏名を全会員に積極的に流すこともしない。

(ニ) 会員が信用情報交換所から入手した情報は、理事会の承認を得た者以外に提供・公開することを許されない。違反した場合は除名または利用禁止の措置がとられる。

(ホ) 役職員には秘密保護の遵守規定を設け、義務づけている。

(3) 某信用販売会社

債権の回収に業務の主体をおいているので、顧客の信用情報の秘密保護には除り意を用いていない。

契約を結んだ企業からの問い合わせにのみ応じているが、秘密保護規定はなく、業者から連絡のあった顧客の不払い情報も、顧客本人に照合されることはなく、そのままカードに記入されている。

(4) 消費者信用共同調査会社設立の動き

通産省のよびかけで、銀行・家庭電気・楽器の三業界が中心となって、消費者信用調査機関設立の動きが活発化している。

出資会社が提供しているネガティブ・リストにより、出資会社からの問い合わせに応ずるものであるが、秘密保護については未だ十分検討されていない。

4.4 対　　策

以上に述べた現状から、必要な対策として考えられることは、つぎのような項目であるが、これらの点については、日本弁護士連合会と緊密に連絡をとり必要な対策を検討する。

(1) 情報処理企業あるいはデータ・バンク側と顧客との間に、個人情報の秘密保護に関して明確に契約条項を定める必要がある。

契約がない場合でも、個人情報が漏洩した場合は、データ・バンク側が民事上の損害賠償責任を負う。

(2) データ・バンク側が顧客に関する新たな情報を得た場合は、必ず顧客本人に照会して確認する。あるいは個人情報の内容を定期的に顧客本人

にプリント・アウトして提示する義務を負わせることを検討する。

(3) 顧客本人から個人情報について訂正の要求があれば、直ちに応じなければならない。ファイル更新との間の時間的ズレによって不利益を蒙ったときは、データ・バンク側の過失責任となる。

(4) データ・バンク側は、問い合わせのあった個人の情報を提供することは差支えないが、収集したいろいろな情報をミックスした総合情報を提供することは禁止さるべきではないか。

5. 技術面からみた秘密保護

電子計算組織の能力が拡大し、大量のデータを高速度で収集し、記憶し、計算し、分類し、検索することができるようになり、また通信回線を通しての遠隔処理システムは時間的、距離的制限を大幅に縮めて、端末装置からのデータの入出力を可能にした。

このような技術の進歩に伴い情報を検索、記憶内容の変更が遠隔地から容易に行なうことができるにおよんで権限外の人間による秘密情報の取り出しや情報内容の変更の可能性が増大した。

電子計算組織の使用に伴う秘密漏洩の可能性の増大がある一方には、電子計算組織そのものの固有の性質から来る安全的役割のあることもみのがすことができない。記憶された特定の情報を取り出したり、機械語を理解するためには高度の技術的知識と機械に対する熟練を必要とし、また電子計算組織の大容量処理能力と、高速性は手作業による処理に比較して、秘密保護に対する用心策を立てやすい一面をもっている。

電子計算組織の導入に際しては、使用者はシステムの特質について、ハードウェアおよびソフトウェア両面からかなりの範囲の選択性を有しており、システム設計の際システムの目的に応じて有効な秘密保護策を採り入れることができる。

必要な秘密保護策の考慮にあたっては、情報の漏洩と権限外の人間による秘密情報への介入による損失、および保護策を実施することによるコストの増加とシステム能率の低下を慎重に評価し、効果的な秘密保護策をシステムに組み込む必要がある。

従来でも、権限外の情報の収集の防止方法として、許可なき者の非報貯蔵区域への立ち入り禁止、権限を与えられる者の選択、秘密資料の取扱い規定等が実際に適用されてきた。

しかし、手作業処理または単独システムに適用されたこれらの方法が必ずしも遠隔処理システムに適用されるとは限らない。従ってそれらの方法を再検討し、新しい時代のシステムに適合するような修正を加える必要がある。ここに大別して次の二つの面から秘密保護に関する具体的な方法を挙げ考察

することにしたい。

5.1 中央処理装置からみた秘密保護策

(1) 記憶区域の仕切

記憶装置に貯えられるプログラムに対して、記憶区域を区切って、割り当てる方法である。特に遠隔処理システムにおいては同時にいくつかの異ったプログラムが存在しており、それらの相互干渉を防ぐ必要からもこの方法は有効である。

(2) 処理終了時の記憶内容消去

処理の終了と同時に記憶装置内部のワーキングエリアの内容を消し去ることも重要である。これを実施しないと新しいプログラムが入れられるまで前のデータとプログラムが残っており、他人による内容の取り出しが行なわれる可能性がある。

(3) 記憶内容の保護

記憶装置に、読み込まれたデータおよびプログラムを他人による変更から守るためにはパスワードにより情報への介入を制限することができる。さらに内容の変更が絶対に許されない性質の情報ならば、非破壊型記憶素子または読み出しのみ可能ないわば一方交通型の記憶素子に記憶させることもできる。

(4) コントロールプログラムの保護

コントロールプログラムの中には安全策を働かせる機能も含むことになるが、これら重要な部分は必要ならば特別の制御用語を使った翻訳プログラムを働かせて、コントロールプログラムを支配させることができる。

(5) 診断用プログラム

故障診断用プログラムは一般にシステムが適切な動作状態にあるかどうかを試すために使われるものであるが、このプログラムの中に意識的に秘密保護策の裏をかくようないくつかの手順を組み込んでおき、保護策が有効かどうかを試すことができる。

この方法によれば機械の故障またはプログラムの欠陥により重要なデ

ータの漏洩をもたらす可能性を未然にチェックすることができる。

(6) システムの稼動記録

システムの使用状況をログするために作られたプログラムは、秘密保護の監視手段の一つとして有効に使うことができる。システムの動作状況を全て記憶しているならば、不法に情報を得ようとしての動作も感知することができる。

(7) 出力資料に対する配慮

電子計算組織からの印刷資料の管理をたすけるため、コピーに一連番号を自動的にふらせるとか、秘密性の度合、取扱い上の指示を書類上に明示することができる。資料に附ずいするデータファイルのラベル、保管指示も電子計算組織から適切に取り出すことができる。

5.2 端末装置からみた秘密保護策

(1) 鍵、パッチカードの使用

権限外の人間による端末装置の使用を防ぐため鍵を取り付ける方法がある。銀行用窓口機械にはこの方法が一般的に使われている。

他に特定のパッチカードを端末装置に挿入したときのみ機械を操作可能にする方法も考えられる。

(2) 端末装置識別コード

端末装置の設置場所により処理可能な範囲を限定することがある。従って重要なデータの入出は特定の端末装置からのみ可能である。役席者端末機がこの例である。それぞれの端末装置は一連の識別コードを電子計算組織に送ることによって区別される。

(3) コールバック方式

端末装置からオペレーターが識別コードを送り出すと、一たん通信回線は切り離され、電子計算組織は内部に記憶している識別コードに対応する回線番号を自動的に選択し、再び通信回線を結合し、業務を開始する。

(4) 個人の確認

端末装置からの呼び出しに応じてコンピュータはオペレーターの識別

番号を要求し、もしその応答が、許可された個人の番号ならば業務の開始が行なわれる。将来は個人の確認は声紋または有線テレビを使って行なうことも考えられる。

(5) パスワード方式

個人の識別番号と同時に個人の権限レベルを確認する方法としてパスワードを使うことができる。種類のちがったパスワードにより、一つは情報の検索を可能にし、他は情報の変更を可能にするといった使い方をすることもできる。

(6) システム監督者の許可を得る方式

保護された情報を取り出す必要がある場合は、処理を中断し、システム監督者に特定種類の情報が必要なことを通知し、情報要求者の権限の承認が行なわれた後、パスワードにより特定の情報の入手を可能にする。

(7) 個人識別番号、パスワードの定期的変更

データファイルが多くの異った秘密保護のレベルを持っている場合、個人の識別番号、パスワードに対応する権限表はある期間内に他に知られるおそれがあるので、その組合せを必要により変更することによって保護策としての効力を保つような配慮も必要になる。

(8) 時間差対策

遠隔処理システムでは問題の入力と結果の取り出しの間に時間的おくれの生ずる場合がある。処理結果を端末側へ送出する前に要求者の在席を確認することが必要となり、またこの逆に処理結果を全て記憶しておき、要求者からの特定の要求により端末側へ送り出す方法もとることができる。

(9) データ伝送中の保護策

情報の伝送にあたっては、内容を暗号化する方法と、伝送エラーを防止するためのチェック機能の採用、および端末周辺における回線のシールドによる盗聴防止などがあげられる。伝送効率を問題にしなければエラー復元可能な伝送コードを使うことも可能である。

6. 管理面からみた秘密保護

ユーザーの秘密保護に関連して、情報処理産業の管理面においても整備を要する問題が多い。

基本的には、管理者が、急速に発達したコンピュータ・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もつことが要請されるが、具体的には人と物の管理という形で把握すべきであろう。

主なる問題点として

(1) 契約条項
(2) 社内規範
(3) 人事管理
(4) 保管方式

等があげられる。

なお、秘密保護に関するもろもろの問題は、委託業務の契約以前の段階、即ち見積り過程あるいは成約準備の段階において、すべてに発生する危険性のあることも充分認識されねばならない。

6.1 契約条項

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。

UNIVERSITY COMPUTING 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を明記したものが多いようであるが、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。

6·2 社 内 規 範

一方、社内規範については下記のような項目についてかな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る。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）

6.3 人 事 管 理

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まだ未熟であり、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、実情にそわないであろうし、斯業育成の大局展望にもそわないかも知れない。しかし、今後進む可べ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、アナリスト、オペレータなど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するといった措置も必要であろう。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。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。

また、情報の性質上秘密を扱う者は非組合員とすると云ったような配慮が民間官公庁の別なく必要であろう。

次に、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傾向がかなり見受けられる。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。

6.4 保 管 方 式

秘密保護の具体的方法として保管の問題が特に重要である。即ち、保管の対象、場所、期間、責任者、損害防止のための遠隔地での二重ファイル、

複製や、又破棄などの問題があげられる。これらの大綱は社内規範にも明示されねばならない。

文書、帳票類の保管はコンピュータ以前の時期にも重要な問題であったが、コンピュータによる大量処理時代には一層周到な配慮を要する。

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厳重な方法で保護されねばならないにもかかわらず、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なくないのである。EDP部門の発展が急であり、会計制度のコンピュータ化などとの均衡ある発展が見られなかったためでもあろう。

米国において、不良のEDP要員が磁石を用いてファイルやプログラムをメチャクチャにした事例が伝えられているが、正に他山の石とすべきである。

さて、保管の場所は重要度に応じ、倉庫、書庫、キャビネット等に施錠保管されるべきであり、出入の記録、重要度に応じた責任者の指定が必要である。また、火災、地震等の不慮の災害に対する措置として遠隔地に二重保管することも配慮すべきである。

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

6.5 秘密保護のための規範

要するに、秘密保護についての管理面の体制が、情報産業の秩序づけと発展のために、競争原理を阻害しない範囲内において、急速に整備されることが望まれるのである。

情報産業の現況はまだ育成の途上にあり、採算上からも直ちに実行困難な点も少なからずあるが、一応管理面から見た秘密保護方策として望まれる規範を具体的に下記に列挙しておく。

(1) 契約に秘密保護の条項を挿入

(イ) 秘密保持の義務条項

第○条　受託者又は受託者の業務従事者は、業務受託者の秘密については、これを他に絶対に漏洩してはならない。

(ロ) 秘密漏洩の賠償責任条項

第○条　受託者又は受託者の業務従事者は委託契約遂行に当たり、受託業務上の秘密漏洩により委託者に損害を与えた時は委託者の被った損害額を賠償する責を負うものとする。但し受託者又は受託者の業務従事者の怠慢でなかったことが立証された時はこの限りでない。

(2) 人事管理面の措置

(イ) 情報秘密保護の責任者の選任

秘密情報の性格上、資格として非組合員とする。

(ロ) 情報処理担当組織

プログラマー、オペレーター、ライブラリアン等の分権体制の採用内部統制組織の確立をはかる。

(ハ) オペレーション操作

オペレータ複数制を条件とする。

(ニ) オペレーション操作資格者

オペレーションは一定の担当者を指定登録し、該当者以外のオペレーションを禁止する。

(ホ) 秘密保護の教育実施

社内秘密保護規定を制定し、（参考資料一例を参照）、社内業務従事者に対し、絶えず教育を実施、徹底を期する。

(3) 情報取扱上の措置

(イ) データーの管理連絡搬送

原始資料及びデータ授受の確認、数量チェック、受渡記録の制度を確立する。運搬には自社運搬車利用を原則とし、鍵付容器を採用する。社内保管は金庫に収容し、使用後の処理の取り極めをする。

（オンライン関係は技術的対策の項参照）

(ロ) 電算機入出力媒体（基礎資料媒体、中間～長短期保存媒体）の取扱。

ライブラリアン制による責任管理体制をとる。保存方法についてはカード、紙テープは耐火金庫に格納、磁気テープ、磁気ディスク類は、重要度に応じ鍵付キャビネット、耐火保管庫に収容し、コピィーを分離保

管する。

(ハ) 作製諸表、文書の取扱

電算機アウトプットデータ及び諸表文書の社内授受体制を明確にする。管理、連絡、搬送については前記(イ)に準ずる。

なお、未使用用紙類についても、社印、社名、アウトプット項目など印刷されたものは上記の扱いに準ずる。

(ニ) 情報処理関係ドキュメンテーションの取扱

システム記述書、ランブック、オペレーションガイド、コードブック等の社内保管、使用方法を制定する。

(ホ) 反古の処置

汚損または用済作表、カード、紙テープ等の廃棄方法を制定する。

(ヘ) コンソールログの取扱

オペレーションの内容をチェックし、電算機不正使用を点検する。操作証拠資料として、保存方法、期間等を制定する。

(ト) 部外者の入室制限措置

事務室、電算機室等秘密事項の取扱われる場所への担当者以外の立入を禁止または規制する

(4) 環境整備措置

(イ) データの保管設備

施錠カードキャビネット、施錠磁気テープ(ディスク)キャビネット、耐火磁気テープ(ディスク)保管庫などを設置する。

(ロ) 機器、データに対する防護設備

炭酸ガス消化装置の備えつけ、　停電装置付電源、電源に対するバックアップ対策など考慮する。

(5) 秘密保護規程

参考資料——社内規程参照。

なお、ミス、不正データチェックの問題については技術的対策の項に譲った。

7. 必要な対策

7.1 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、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、憲法など幅広い法制的検討を要するものであるので、本項においては、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し、プライバシーの保護については、日本弁護士連合会とも連絡をとりつつ別途さらに検討をすすめることとする。

7.2 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ェア、ソフトウェ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ェック方式と同様に、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　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。」

7.3　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な誘導的な措置がとられることが望ましい。

7.4 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

これは、強制的なものでなく、情報処理サービス業、情報提供サービス業を営む者に、或はこれを利用する人々に秘密保護のためにとるべき措置の規範を提示し、啓蒙してゆこうとするものである。

具体的な内容は、既に5、6章において述べられているので項目のみを掲げることとする。

(イ) 技術上の秘密保護措置の啓蒙

5章に示した技術的手法について啓蒙普及する。

(ロ) 契約に秘密保護条項を導入

- 秘密保護の義務規定
- 秘密漏洩の損害賠償規定

(ハ) 人事管理上の措置

- 責任者の選任、非組合員化
- 職種別分権体制の確立
- オペレーターの資格化
- オペレーターの複数化
- 秘密保持規程の制定と教育

(ニ) 情報取扱上の措置

- データの授受、搬送の管理
- 電算機入出力媒体の管理
- 文書等の管理
- 反古の処置
- コンピュータ・コンソール・ログの管理
- 入室制限

(ホ) 環境整備

- データの保管設備
- 機器、データの防護設備

(2) 情報処理技術者認定制度の活用

これは、昭和44年度から開始される情報処理技術者認定制度において管理者レベルの技術者が対象になった場合に、試験範囲に秘密保護の技術手法、管理手法の科目を加え、秘密保護について正しい知識をもつた技術者を育てる。

(3) 情報産業を営む事業者の任意登録制度の創設

これは登録を事業を営む要件とするのでなく、優良事業者を登録させ、その旨の表示を許すもので、利用者からのクレームを受付け、一定要件を欠くにいたった時は登録を取消すというものである。登録要件に、秘密保護の技術上の措置、管理上の措置がとられていることを加えれば、目的を果たせることになる。

付　属　資　料

1. 技術面における秘密保護のための要素

2. 技術面における秘密保護の手法

1. 技術面における秘密保護のための要素

コンピュータを利用して、大量・高速のしかもその中間過程が目に見えない処理が多くなるにつれ、新しく外部との接触が増加する。

外部との接触の増加に加えて処理能力の増大、管理資料の細分化などから、秘密に関しての保証または安心感がなければ、外部処理がいかにコスト的に有利になっても踏み切ることはできない。

今回の技術面における秘密保護に対する手段は、広く情報処理サービス業、情報提供サービス業が発展するためには、節度ある処理の必要性が十分察知され、技術的にも解明され始めているのでこの問題を深く彫り下げることである。

しかし、この分野の先進国であるアメリカにおいても、法的には契約履行、契約不履行についての争いはあっても、公共的には確立されたものはない。

アメリカでの大項とわが国で考えられる技術をこゝに紹介することによって、参考になれば幸甚である。

秘密保護を考慮すれば、当然、単純処理よりもコスト高になるが、これをできるだけ増加させないで、しかも、自動的にミスを発見できるシステムが望ましい。

その要素としては、次の5通りの中から発生し、防止する必要がある。

1. ハードウエアによる
2. ソフトウエアによる
3. 環境整備による
4. 防止方式による
5. 人材育成による

それに対して現在では漏れて問題を起したケースは情報処理サービスでは殆んどないが、内部処理ではすでに発生している。

その対策として考えられる方法を列挙すると次のようなものがある。

1. 中央処理装置に異常発生を知らせる探知方法
2. 命令の横取り
3. マルティ・プログラミングにより高速処理されると、データを盗用す

ることはその過程では難かしい。

4. ファイルにマスクをかけ、制御用言語で固有の言葉を作る。
5. コードをユーザーが組み合せて使用するファイル・コードの利用。
6. ファイルの内容を変更する場合には特定の場合だけとし、事前に伝達されるようにする。
7. ファイルの取り外し時間を決める。
8. 他人にわかりにくいラベルをつけ、チェックする。
9. データを入力する形式を指定する。
10. ターミナルでは処理プログラムと制御プログラムを区分しておく。
11. ターミナルにキイ・コードだけで作動するようにする。
12. キイ入力によってコード変換され、場合によってロックできるようにしたもの。
13. ハードウエアとして、コード変換不能の回路制御をする。
14. ユーザーと内部コードとの両方がキイになるようにする。
15. パスワードを作る。
16. コードの入ったバッヂで人を区分する。
17. 暗号を使用する。
18. データと人のコードともにパスワードを使用する。
19. キャラクタを変換して盗聴防止をする。周波数を変える。
20. ダイヤルを一度切って逆探知する。

これらの対策を含めて実際の秘密保護を考慮したシステム素案を考えることにする。

1. データ作成過程の考え方

一般に、大量データになると数多くの入力方法を組合せて作成することが多くなり、為に、パンチだけとか紙テープ作成用のタイプだけではなくなってくる。

そのためには秘密保護の方法も均一に考えることはできない。

しかも、データ作成過程では従来の手書き処理と異って、分類基準にもとづくコードを挿入するコーダー、その伝票を見てパンチまたはタイプす

る人々、さらに、機械室でのオペレータ、プログラマー、チェッカー、管理者まで余分にデータを見るチャンスをもっている。

少なくとも、性悪説にたてばこの過程が手作業より増加するだけ秘密保護はむずかしくなる。

したがって、第1の考え方は中間媒体作成者が少ないほどよいということになる。

2. バッチ単位のチェック

1日単位とか100枚単位ごとに1連番号として処理し、1連番号と正味口座は別の照合をして処理されるようにする。

例えば、選果場にもち込まれるみかんやりんごは、同一のかごで納入して選考員が優劣を決めているが、納入者氏名が明記されていると、漏れや片寄りを生ずる恐れがあるので受付で1連番号にし、その評価結果と正味口座名が照合されるケースが多い。

この方法は、機械的には納入業者のデータを直接使用されない損失はあるが、逆に氏名を知ることによっての談合を防ぐことができる効果をもっている。

3. 答案とじ

すでに実施段階に入ったものに各種試験の採点の機械化がある。

例えば、人事院の公務員任用試験に対する模擬試験では、氏名によって採点者に歪みがでては困るし、手心を加えてはさらに問題である。

そのため、従来からも答案を上片だけ綴って、氏名や受験番号を可視できないようにして採点されている。

これと同じ方式をマーク・シートで行ない、答案とじした答案を機械室に持ち込み、機械室で開封して係員立合いで処理する。

機械に入力される段階になれば、氏名が解読できてもスピード的には改ザンは不能であるし、氏名と採点結果とは分離されて最高点から順に受験番号と内容がリストされ、この過程でも秘密は保護される。

この考え方を販売、経理伝票のデータ作成に利用すれば、秘密は保護さ

れる。

この考え方を販売、経理伝票のデータ作成に利用すれば、秘密は保護される。

そのような帳票設計が必要となる。

4. 分散発注

個々の売り上げ伝票の内容が漏れることがあっても、月日別、品目別、数量であろう。この場合地区別とか、取引店別、売上数量や、リベート率が漏れることは望ましくない。

これに対処するため新聞用紙の発注を分散し、発行部数が推定されないようにするのと同様に、3カ所またはそれ以上に量をかえて、発注してデータ作成をさせれば、まとめられた時点でなければわからないことになる。

パンチ、マークなどの外注に適している。

5. ネーミング

コード化することは機械処理を前提としたネーミングである。

したがって、名称のつけ方は秘密保護のみならず、処理過程のチェックにも異常の検出にも使用される。

ニューモニック・コードは、本人もまた外部の人々でも解読できるので、プロジェクト名がわかるだけでも問題になることがある。

例えば、ある企業が輸送手段別の価格予測を依頼したとすれば、それだけで、ライバル会社にとっては、内容よりも実施しようとすることがわかるだけでも価値あるものである。

そのために、ネーミングとして解読できるものはオペレーショナルな業務であって、その他は暗号コード（Cryptography）が望ましい。

アメリカの貸金庫では毎日その都度ナンバーをかえてセットできるものがある。

このように、業務についても暗号化と機械処理の容易性およびチェック可能なネーミングが望ましい。

ナンバー・コードにチェックする機能をもたせると、次のようなものが

ある。

6. オペレーションの保護

付属資料2のオペレーションの保護の項参照のこと。

および、ＣＩＮのプリント表1参照のこと。

7. 流れ図の記号化

フロー・チャートと呼ばれる業務処理の流れ図は人によって異なり、特に細部にわたって克明に記載する人と概略図にとどめる場合がある。

しかし、最終段階では機械語となり、その解読は8進法や2進法の場合殆んど他人が見てもわからない。

それに対して、アセンブラー・レベルならば、やゝプログラムを理解している人々なら解読可能であるが、流れ図がなくては読みとることはむずかしい。

そこで、流れ図を標準化するとともに、プログラム改訂にも役立つオート・フロー（プログラムを挿入するとコンピュータが流れ図をプリントし、不備な個所を指適してくれるソフトウエア）を利用すれば、コーディング・チャートと合わせて見ればよくわかる反面、片方だけでは意味がわからないので一方を保存し、改訂の都度入れ替えればよいことになる。（図1）

これは、コーディング・シートとフロー・チャートを別個に保存して、一方的に改訂できないようにすると同時に、標準化することで保持される。

8. パラメータの設定

フロー・チャートからプログラム作成としてコーディングする際、業務の流れにしたがって作成すると極めて冗長なプログラムとなる。

そこで、技術的にはプログラム工数の少なくなるように組み立て方を替える必要がある。

この場合、パラメータを利用して逐次変更できるようにすることが多い。

そして、このパラメータは暫定として使用し、本番で真実の係数が入れられるようにすれば方法論は漏れても実質的には秘密が保持される。

例えば、リベート率とか信用限度の算出審査基準、オーダー・ポイントなどである。

この場合の問題点は、デバッグの際に使用するテスト・データと疑似パラメータとの間から算出される結果が、現実に使用するものとかけ離れた数字になることであるが、なれれば問題ではなくなる。

9. ラン・ボタンとセンスキイ

コンピュータを稼働させるには、これから仕事を始めるという「スタート」を示すラン・ボタンを押して始まる。

または、どの部分にスイッチせよという命令にしたがって稼働中新しい業務に移行する。

いわゆるセンス・キイである。

このいづれかに指示されない限り稼働しないので、この点を配慮したシステムが必要であり、それにはハードウエア自身と、ソフトウエア、それに複合されたファームウエアによって制御することができる。

10. 記 憶 保 護

メモリー・プロテクションによって、事前に記憶されている内容を破壊されることはなくなった。

と同時に、場所指定された部分だけが保護されることから、アドレス別の検索回数を確認することができる。

特に、人事情報とか財務情報の特定の部分だけが多くリクエストされることが増えれば、異常を探知することができる。

そのためには、事前に若干のソフトウエアを準備する必要がある。

これはその1例である。

アドレス別の最初の状態を1とすれば、n回検索される中のAアドレスが検索される平均はn／Nである。

1定期間に特定アドレスが平均よりどれだけ急激に増加したかは増加率で探知し、平均以下のアドレスでも急に平均値に近づくことも異常探知となる。

図1　オート・フローによる流れ図（例）

```
* * * G69154  .PRI      FLOW
        67310
             LBC       FLOW     DISR   EDP          000001     01   NNNNY
             LBC       FLOW     DISO   EDP          000001     01   NNNNY
             LBC       FLOW     DISS   EDP          000001     01   NNNNY
             END
                       1499 * END OF PROGRAM LOAD

HDR1EDP          0000010001   F114264G69154G69154S140158000000000000000000000000   *DISC FILE LABEL*
HDR1EDP          0000010001   F114264G69154G69154S140158000000000000000000000000   *DISC FILE LABEL*
HDR1EDP          0000010001   F114264G69154G69154S140158000000000000000000000000   *DISC FILE LABEL*
HDR1EDP          0000010001   F114264G69154G69154S140158000000000000000000000000   *DISC FILE LABEL*
```

表1. CIN法によるチェック・レター

		W	055 M	121 Q	187 H	253 B	319 W	385 Y	451 J	517 M	583 N	649 Y	715 P	913 V	847 T	781 H	979
		X	056 N	122 Z	188 A	254 G	320 X	386 Z	452 T	518 N	584 K	650 Z	716 Q	914 E	848 U	782 X	980
		Y	057 P	123 S	189 B	255 V	321 Y	387 S	453 U	519 P	585 G	651 S	717 R	915 F	849 V	783 L	981
		H	058 Q	124 X	190 C	256 W	322 H	388 T	454 Z	520 Q	586 H	652 B	718 J	916 C	850 W	784 M	982
		A	059 R	125 L	191 D	257 X	323 A	389 U	455 N	521 R	587 A	653 C	719 K	917 Z	851 X	785 N	983
		E	060 J	126 M	192 N	258 Y	324 F	390 V	456 P	522 S	588 B	654 H	720 U	918 S	852 Y	786 P	984
		U	061 K	127 N	193 P	259 Z	325 U	391 W	457 Q	523 T	589 C	655 W	721 V	919 T	853 Z	787 Q	985
		V	062 U	128 P	194 L	260 S	326 V	392 F	458 R	524 Y	590 D	656 X	722 S	920 U	854 A	788 R	986
		W	063 V	129 Q	195 H	261 T	327 W	393 G	459 J	525 M	591 E	657 Y	723 P	921 V	855 B	789 J	987
	END	X	064 S	130 R	196 A	262 C	328 X	394 D	460 K	526 N	592 P	658 Z	724 Q	922 W	856 G	790 T	988
		Y	065 P	131 J	197 B	263 D	329 Y	395 S	461 L	527 P	593 Q	659 S	725 R	923 X	857 V	791 U	989
C	000	Z	066 Q	132 T	198 C	264 A	330 Z	396 T	462 V	528 Q	594 M	660 T	726 J	924 G	858 W	792 Z	990
Z	001	S	067 R	133 U	199 D	265 X	331 S	397 U	463 W	529 R	595 A	661 U	727 K	925 H	859 X	793 N	991
S	002	B	068 J	134 R	200 E	266 Y	332 B	398 V	464 T	530 J	596 B	662 D	728 L	926 E	860 Y	794 P	992
T	003	C	069 K	135 E	201 F	267 Z	333 C	399 W	465 Q	531 K	597 C	663 E	729 M	927 T	861 Z	795 Q	993
U	004	H	070 L	136 F	202 Q	268 S	334 A	400 X	466 R	532 U	598 D	664 B	730 W	928 U	862 S	796 R	994
V	005	W	071 M	137 G	203 R	269 T	335 X	401 Y	467 J	533 V	599 E	665 Y	731 X	929 V	863 T	797 J	995
W	006	X	072 W	138 H	204 N	270 U	336 Y	402 H	468 K	534 J	600 F	666 Z	732 U	930 W	864 C	798 K	996
X	007	Y	073 X	139 A	205 B	271 V	337 Z	403 A	469 L	535 F	601 G	667 S	733 R	931 X	865 D	799 L	997
G	008	Z	074 C	140 B	206 C	272 E	338 S	404 F	470 M	536 G	602 R	668 T	734 J	932 Y	866 B	800 V	998
H	009	S	075 Z	141 C	207 D	273 F	339 T	405 U	471 N	537 H	603 J	669 U	735 K	933 Z	867 Y	801 W	999
V	010	T	076 S	142 M	208 E	274 L	340 U	406 V	472 X	538 A	604 P	670 V	736 L	934 A	868 Z	802	
J	011	U	077 T	143 N	209 F	275 H	341 V	407 W	473 Y	539 B	605 C	671 W	737 M	935 B	869 S	803	
K	012	D	078 U	144 A	210 G	276 A	342 E	408 X	474 D	540 C	606 D	672 F	738 N	936 G	870 T	804	
L	013	E	079 V	145 X	211 H	277 B	343 F	409 Y	475 S	541 D	607 E	673 G	739 P	937 V	871 U	805	
M	014	U	080 W	146 Y	212 J	278 C	344 T	410 Z	476 T	542 N	608 F	674 M	740 Y	938 W	872 V	806	
N	015	R	081 X	147 Z	213 K	279 D	345 Q	411 S	477 U	543 P	609 G	675 A	741 Z	939 X	873 W	807	
P	016	J	082 G	148 S	214 H	280 E	346 R	412 B	478 V	544 B	610 H	676 B	742 E	940 Y	874 F	808	
Q	017	K	083 H	149 T	215 W	281 F	347 J	413 C	479 W	545 Y	611 A	677 C	743 T	941 Z	875 G	809	
Z	018	L	084 E	150 U	216 X	282 Q	348 K	414 S	480 X	546 Z	612 K	678 D	744 U	942 S	876 U	810	
S	019	M	085 T	151 V	217 Y	283 R	349 L	415 P	481 Y	547 S	613 L	679 E	745 V	943 T	877 R	811	
X	020	N	086 U	152 E	218 Z	284 N	350 M	416 Q	482 H	548 T	614 A	680 F	746 W	944 C	878 J	812	
L	021	P	087 V	153 F	219 S	285 B	351 N	417 R	483 A	549 U	615 X	681 G	747 X	945 D	879 K	813	
M	022	Y	088 W	154 C	220 T	286 C	352 X	418 J	484 F	550 V	616 Y	682 R	748 Y	946 T	880 L	814	
N	023	Z	089 X	155 Z	221 U	287 D	353 Y	419 K	485 U	551 W	617 Z	683 J	749 Z	947 Q	881 M	815	
P	024	W	090 Y	156 S	222 D	288 E	354 V	420 L	486 V	552 F	618 S	684 P	750 A	948 R	882 N	816	
Q	025	K	091 Z	157 T	223 E	289 F	355 J	421 M	487 W	553 G	619 T	685 C	751 B	949 J	883 P	817	
R	026	L	092 A	158 U	224 B	290 G	356 K	422 W	488 X	554 D	620 U	686 D	752 G	950 K	884 Y	818	
J	027	M	093 B	159 V	225 Y	291 H	357 L	423 X	489 Y	555 S	621 V	687 E	753 V	951 L	885 Z	819	
T	028	N	094 G	160 W	226 Z	292 J	358 M	424 U	490 Z	556 T	622 E	688 F	754 W	952 M	886 W	820	
U	029	P	095 V	161 X	227 S	293 K	359 N	425 R	491 S	557 U	623 F	689 G	755 X	953 N	887 K	821	
Z	030	Q	096 W	162 G	228 T	294 Q	360 P	426 J	492 B	558 V	624 C	690 H	756 Y	954 X	888 L	822	
N	031	R	097 X	163 H	229 U	295 D	361 Q	427 K	493 C	559 W	625 Z	691 A	757 Z	955 Y	889 M	823	
P	032	S	098 Y	164 E	230 V	296 E	362 Z	428 L	494 H	560 X	626 S	692 K	758 S	956 V	890 N	824	
Q	033	T	099 Z	165 T	231 W	297 F	363 S	429 M	495 W	561 Y	627 T	693 L	759 T	957 J	891 P	825	
R	034	D	100 S	166 U	232 F	298 G	364 X	430 N	496 X	562 H	628 U	694 R	760 C	958 K	892 Q	826	
J	035	S	101 T	167 V	233 G	299 H	365 L	431 P	497 Y	563 A	629 V	695 E	761 D	959 L	893 R	827	
K	036	T	102 C	168 W	234 M	300 A	366 M	432 Y	498 Z	564 F	630 W	696 F	762 A	960 M	894 S	828	
L	037	U	103 D	169 X	235 A	301 B	367 N	433 Z	499 S	565 U	631 X	697 G	763 X	961 N	895 T	829	
V	038	V	104 A	170 Y	236 B	302 L	368 P	434 E	500 T	566 V	632 G	698 H	764 Y	962 P	896 Y	830	
W	039	W	105 X	171 Z	237 C	303 M	369 Q	435 T	501 U	567 W	633 H	699 A	765 Z	963 Q	897 M	831	
B	040	X	106 Y	172 A	238 D	304 J	370 R	436 U	502 D	568 X	634 N	700 B	766 S	964 Z	898 N	832	
Y	041	Y	107 Z	173 B	239 E	305 F	371 J	437 V	503 E	569 Y	635 B	701 C	767 T	965 S	899 P	833	
Z	042	H	108 S	174 Q	240 F	306 G	372 T	438 W	504 B	570 Z	636 C	702 M	768 U	966 F	900 Q	834	
S	043	A	109 T	175 D	241 G	307 H	373 U	439 X	505 Y	571 S	637 D	703 N	769 V	967 U	901 R	835	
T	044	W	110 U	176 E	242 R	308 A	374 H	440 Y	506 Z	572 B	638 E	704 K	770 E	968 V	902 J	836	
U	045	K	111 V	177 F	243 J	309 B	375 W	441 Z	507 S	573 C	639 F	705 G	771 F	969 W	903 K	837	
V	046	L	112 E	178 G	244 E	310 C	376 X	442 A	508 T	574 R	640 G	706 H	772 C	970 X	904 U	838	
W	047	M	113 F	179 H	245 T	311 D	377 Y	443 B	509 U	575 E	641 H	707 A	773 Z	971 Y	905 V	839	
F	048	N	114 V	180 A	246 U	312 N	378 Z	444 X	510 V	576 F	642 J	708 B	774 S	972 Z	906 A	840	
G	049	P	115 J	181 B	247 V	313 P	379 S	445 L	511 W	577 G	643 K	709 C	775 T	973 S	907 X	841	
D	050	Q	116 K	182 L	248 W	314 D	380 T	446 M	512 F	578 H	644 F	710 D	776 U	974 B	908 Y	842	
S	051	R	117 L	183 M	249 X	315 S	381 U	447 N	513 G	579 A	645 U	711 E	777 V	975 C	909 Z	843	
T	052	S	118 M	184 J	250 Y	316 T	382 D	448 P	514 W	580 B	646 V	712 P	778 W	976 Y	910 S	844	
U	053	T	119 N	185 F	251 Z	317 U	383 E	449 Q	515 K	581 C	647 W	713 Q	779 X	977 M	911 T	845	
V	054	Y	120 P	186 G	252 A	318 V	384 B	450 R	516 L	582 M	648 X	714 E	780 G	978 N	912 U	846	

したがって、微分係数によってチェックすることができる。

この場合は、主にオンラインのリクエストに多い。

記憶保護の思想は多重処理におけるプログラムを含む破壊を恐れ、安全を計るハードウエアであるが、本来ソフトウエアのために必要となった機能とみなせる。

11. ソフトウエア

一般に、業務の開始はスタートのサインが必要であり、その事前にロックされることを考えることがソフトウエアの技法の中心となる。

コンピュータに電源をＯＮさせて、安定状態になるまではスタートできないが、その間は機種構成によって５秒～３０分である。

正常な状態が確認されると、破壊式の記憶装置にはプログラムまたはデータを挿入し、作動準備完了となる。

また、非破壊式記憶ならば即座に準備完了となる。

信頼されたオペレータによって遂次進行されるが、この間に秘密が保護できない場合は、ソフトウエア技法でカバーしなければならない。

タイム・シェアリング・システムでは、記憶装置に入る前に通信制御機構が働き、ハードウエア的に処置される。

この場合、緩衝記憶を含めてソフトウェアで解決することもある。

チェック方式はパスワードともいうべきもので、条件にあわない場合は除外されるようにコードを作る。

一般にはチェック・コードである。

12. 間接アドレス方式の作動

ソフトウエア的に最も信頼されるのは、間接アドレスを利用して本人または登録番号を知っているもの以外には、作動開始命令につながらないようにする。

すなわち、比較・係数・論理を通じて所定のスタート・アドレスに導びかれれば、そのまゝスタートできるが、それ以外はスタート・アドレスに到達しないので、リジェクトされるようにするわけである。

最近のコンピュータは、殆んど全べてこの方式でソフトウエアを作成することができる。

13. 制御補助装置

ハードウエアで上記のことをするには、通信制御に用いるスイッチング・コントロールとかポーリングの技術によって、自動的に、特定入力以外は除去することができる。

この場合にも、ネーミング・コードにキイがなければならない。

14. ファイル・マスク

探知すべきファイルに対しては、ファイル・アドレスの番号がわからなければならない。この場合に、ファイルの1部にマスクをして穏された番号を追加しないと、正しい制御用言語にならないように仕組むことができる。

また、ファイルに固有のコードを付して、その都度変更することもできる。

15. ファイル・コーディング

一部を穏してそれを追加すれば正常になるファイル・マスク方式に対して、ファイルを指示する番号は組合わせないと作られないようにした方式である。

アメリカの貸金庫の一部にもこの方式を採用している。

16. コントロール・ログの保護

コンピュータの中央制御装置からは、その進行状態をディスプレーまたはタイプで表示される。

表示の点滅だけでは制御できないので、連続用紙にプログラマーやオペレーターとの対話形式で印字される部分が、コントロール・ログまたはコンソール・ログである。

現在このログは、オペレータが自由に取り替え、行替え、挿入ができる

ようになっているが、銀行で使用している窓口機械は出納者の鍵によって番号が印字され、その後の時系列経過を改ザンすることができないようになっている。

この装置をもつことによって、出納者に支払権限が委譲したように、このコントロール・ログをテラーズ・マシンのような装置に付加すると、オペレータやプログラマーによる機密の漏れはなくなり、リモートでも進行状況を把握することができるわけである。

17. 逆探知装置

リクエストが盛んになり、また、リモートで処理できることはそれだけ多くの人々によって操作できるようにしたものである。

電話電報のように、発信者を逆にダイヤルで確認してから受けるのと同様に、端末から発信される番号を自動的に逆探知して正しければ継がるようにすれば、ネームと端末番号の両面から確認することができる。

18. 時 間 指 定

あらかじめスケジュールを決め、その時以外にはリクエストとかオペレーションを不能にする行為である。

計算センターの場合には、その時間だけ立ち合って処理する方式になる。

19. フォール・バック・システムの必要性

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

しかしこの方法では、例えば、ネーミングかコードが診断されて不正となれば、機械が稼働すること自体を停止してしまう。

その後から、不正個所を訂正して再スタートするのが本来であった。

それがもし頻発するならば、むしろ診断して不適正部分を除去し、次のリクエストなりオペレーションに応じられることが望ましい。

シングルのシーケンシャル処理用コンピュータでは、その間に訂正して鉄み込むわけには行かない。

そのために、不正のリクエストが起るたびに機械を止めて、補修してから処理することになってしまう。

この方法では、オンライン時代のリアル・タイム処理は、実質的にはできないことになる。

そこで考えられたのが、フォール・バック・システムというソフトウエアである。

不正を発見すると、コンピュータを停止することなく進行させる方式である。

これは不正に対して生れた技術ではなく、故障に対応するために作られたものであるが、コントロールの立場からは同等に扱かっても差しつかえがないと思われる。

データをソフトウエアでチェックすると、その論理にかなわないときは、データが誤って入力されたか、プログラムに誤りを生じてきたのか、機械が故障したのかを即断することはできない。

したがって再入力する。この場合にもし第1回目と第2回目が異っていて、第2回目が論理通りならば、第1回目に入力したときのデータは読みとりエラーか、第2回目が読取りエラーであるので、もう一度行ない第2回目と同じならば次に進む。しかし、第3回目が異なれば、データの誤りではなくむしろプログラムか機械の故障となるので、この場合プログラムを再スタートして同じデータを読む。

そして、論理にかなえば、プログラムがデータの影響で変化したことを知らせると同時に進行を次に移す。

そして、データ、プログラムともに欠点が発見されるためには、バイオレーション・プログラムと呼ばれる回復プログラムを作成しておく必要がある。

このフォール・バック・システムは、データが故意に歪められても、データに誤りを生じても、プログラムに支障が起きても、また、機械が故障しても、ただちに回復できるようにするソフトウエアで、リアル・タイムシステムでは欠くことのできないものである。

しかし、秘密保護の面から考えれば、さらに論理的に異常探知とかプロ

グラム破壊を防止することが必要である。

20. 割り込みのチェック

新しいコンピュータには割り込みが可能なハードウエアが多い。

この過程でのデータ追跡とか誤りの発見または秘密保護はむずかしいが、次のようなことがすでに行なわれている。

1) 割り込みが行なわれると、それ以後の割り込みを優先ルーチンが完了するまでは使用できないような装置をつけるか、ソフトウエアで処理する。

2) 割り込まれた時の位置を記憶しておき、優先ルーチンが完了するとその時点に戻れるように装置として仕組まれている。

3) レジスタの内容を保存して回復できるようにする装置またはソフトウエアを作る。

4) 割り込みの原因または目的を確認したり、どのチャンネルから割り込んできたかを確認するための装置、この場合は、通信制御装置に似たものを付加するかソフトウエアで処置する。

5) 連続して処理するかどうかをチェックするのは、ソフトウエアで行なう。

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ための装置を付加するか、またはソフトウエアで処理する。

以上は割り込みのある場合で、マルティ・プログラミングやマルティ・プロセシングといわれる多重処理ではこの考え方が必要である。

もちろん、逆に多重処理になると命令やデータを盗みどりすることは殆んど不可能になる。

というのは、ある時点において、その目的とするデータや命令がどこにあるかは、プログラマーにもわからないほどだからである。

むしろ、出力されたときに秘密が保護されないので、出力にその重点を置けばよい。

この優先ルーチンとフォール・バック・システムを組み合わせれば、イギリス銀行のオンライン・システムのように犯罪防止手段に使用できるこ

とは当然である。

実施に当って

コンピュータを直接利用できる人は、事前に認可制をとる。

この場合、端末の操作、コンピュータの中央制御装置、外部記憶装置または媒体がその対象となり、その結果、出力されるのでこれらにたづさわる人々の登録と認可が第一条件になる。

認可された人々は、各々固有の番号が与えられ、適宜変更していく。

マサチューセッツ工科大学のＭＡＣ計画では、端末を利用できる人には１０桁のアルファベットを含むコードが与えられている。

そして、与えられた端末からのみ、そのコードが挿入できる。

この場合、タイプライタを使用しているのでその番号が印字され、事後、盗用される恐れがあるのでコンピュータからその番号をＯＫと確認すると、その番号が印字された上に再び別のコードが重ねられて印字されるので、解読ができないようになっている。

しかも、１０桁のアルファベットを含む数字コードは、他人が容易く憶えることも困難にしている。この番号がＯＫになると、次にその認可者が利用できる範囲の記憶部分が与えられ、それを越えた領域については、記憶装置を利用できないようにソフトウエアで処理する。

この方法は、認可者に対する認可事項表を通過してから作動するので、その他の領域が指示されると要求した認可者番号と、要求する取り出し内容はコンピュータに自動的に記録できるようにして、調査の対象になるか誤って指示したのかを確認する。

したがって、認可者コード・端末コード・要求内容によって正しく使用されているかどうかを、バイオレーション・プログラムという異常探知確認用ソフトウエアで検出されるわけである。もちろん、端末コードとの連繋はハードウエアによるチェックも行なわれる

一般に監査追跡といわれるAudit Trailは、追跡可能になる範囲のデータをコピーし蓄積するので、モニターによって即時検出も優先順位によっては、後日解析にも利用できるように設計される。

このように、実施に当っては一応秘密保護の方法はあると考えてよい。

しかし、前述のような認可者の番号制度、ファイルの符号化、盗聴されてもわからないようにデータを移送中にはパック（集約）する方法などのソフトウエア技術と、端末・制御・記憶における保護とか、検出装置としてのハードウエアの両面から考慮しなければならない。

現在の技術では盗聴に対するものがやゝ不備であるが、他の方法と合わせて実施すれば一応防護できるものである。

コンピュータと通信に関するＢＥＭＡの回答では次のようになっている。

「通信ケーブルや電力ケーブルを物理的にシールドして、外部に漏れないようにするための費用は極めて高価であるから、盗聴によるシステムの侵入を防ぐ有効な手段はみつからない。

しかし、盗聴にたいする弱点を軽減するのには役立つ方法がある。

○盗聴する人は、特定のデータを得ようとすればシステムがどのように作動するかについて、相当の知識をもっていなければならない。

したがって、システムの資料を入手できないように制限することはできる。

（注）　システム・プログラマーとオペレータの分離とか符号化については、認可者登録制にして一致した別コードが検出された時だけ、別のコードに変えるように指示するプログラムの開発によって、たとえ知識をもった人が盗聴しようとしても、３つ以上の組合せがＯＫにならなければわからないように組立てる。

- ○　端末装置の応答機能と符号化されたコードの組合わせによって妨害できる。
- ○　ファイル、データを符号化すれば単純な盗聴は防げる。
- ○　検出用プログラムは盗聴者の活動を検出するのに役立つ。
- ○　機密対話用周波数変換装置にすれば、盗聴者に対して傍受データを役立たぬものにする。

端末装置やコンピュータ、伝送線に存在する誘導磁界もまた、安全問題

に関係する。多くの進歩した端末装置は、陰極線管によるインフォーメーション・ディスプレイを使っており、ある場合には、これらの磁界は重要なシールドおよび電気的漏洩の問題を惹起する。安全確保のためには端末機が置かれている建物、または部室の物理的シールドを行なわなければならない。

コンピュータと電子機械的端末装置もまた、数マイルの距離からでも検出することができる電磁波を放出している。この場合には雑音を発生させることによってデータを読取り傍受不能にすることができる。」

とある。

この他、識別として、音声で一連のコードを作成し他人の使用を押えたり、クレジット・カードに指紋と組合せて識別することも考慮され始めている。

2. 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、しかし、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、デバッグ過程で起こ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-checking 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。

(1) 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。

(2) リダンダンシー法

NCRのチェック・ディジット・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

各桁に異な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。

(3) 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

07、14、21、28、35、42、49、56、63、70

余りを利用することによってチェック・ディジットとして使用できる。

(4) オッド・イーブン法

1　2　3　4　5　3　　9 － 6 ＝ 3

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。

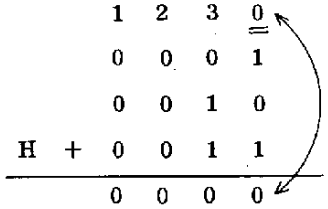
(5) ＣＩＮ法

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、ディジットでは、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。

(6) オート・コレクション法

この方法は、情報理論を用いて、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こ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。

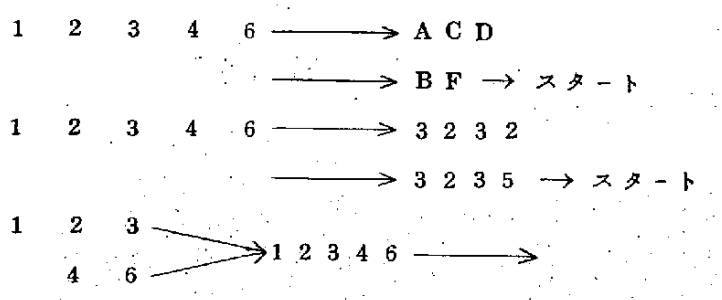
(6) 機械をストップする。

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。

まず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6,１００万円をも着服したし、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ークエンス・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な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1,800万円までは、36,000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。

海　外　文　献

I　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

2. コンピュータとプライバシーの法律

3. コンピュータ・システムにおける安全と秘密

4. 情報の機密性に関するシステムのかかわり合い

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・パ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。

わが国で現在起こりつつあり、また将来起こ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づいた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、顧客の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、それによって起こ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。由々しい結果が起こり得るのだ。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こ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づいて、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 ── 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年ウイ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 ── 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こし得るだろう。

最近の状況から予測すると、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こ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示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

権限のない外部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タの責任に対して、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。禁示命令は、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こる。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こったときには、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、この法律条項に対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) プリント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「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も失敗しても、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。それは一般の憤激を買うだろう。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 ── 犬や事業や結婚の ── 、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ピーを送るだろう。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事実である。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」にウォーレンとブ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 ── 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、少な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、軽蔑を起こ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こ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進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を見るように、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、誰も盗聴しようとしなくなる。

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。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た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こ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、少な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れられない。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、ページをつき合わ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。

3. コンピュータ・システムにおける安全と秘密

ウイリアム・ウェア
ランド・コーポレーション
サンタモニカ・カリフォルニヤ

序　文

共同利用（リソース・シェアリング）コンピュータ・システムにおける情報の漏洩

数人のユーザー、あるいは数個の問題で、機器構成を共通に持つコンピュータ・システムが現われると、一人のユーザー、あるいは一つのコンピュータ・プログラムからの情報が、もう一人の、あるいはもう一つのプログラムにつなげられるという危険が出てくる。情報が軍事上の機密をふくんでいたり、あるいは何らかの理由で、取り扱いに慎重でなければならない場合は多い。従って、情報が漏れるのを防ぐための安全措置がとられねばならない。ここでは、コンピュータにある情報が過失により、あるいは計画的に、権限を持たぬ者に漏らされる場合をいっているのである。

軍事上、あるいは防衛上の情報を入手しようとするスパイ行為は、たびたび報道されている。コンピュータ・システムは、現在、広く軍事、防衛関係の設備に用いられているので、そのようなコンピュータ・システムに入り込もうとする企ては、未然に予知されねばならない。そのようなコンピュータシステムの情報を守るための安全措置が考慮される必要がある。産業界にも同様の状況がある。多くの企業に関する情報が、特許の工程や技術、その企業の盛衰・実情と関連があるために、社内の機密になっている。ある企業が競争相手のコンピュータ・システムに対して、産業スパイの行為をとることが、利益に結びつくことは想像されうることである。同様に、コンピュータに保存されている個人に関する秘密の情報が、それを入手することを許されていない人々に対して、利益になりうるという状況も想像される。このように、軍事とは無関係の情報に対しても、入り込もうとする企てがなされるこ

とが考えられるのである。

ここでは、共同利用システムに対して、スパイ行為の企ての有無を論じようというのではない。それよりむしろ、この問題は、仮に、現実にはないとしても、少くとも理論的にはあると仮定して、この論文ではこの問題の技術的な面と、安全措置の有効なとり方について論じるだけにする。

第一に用語をはっきりしておく。軍事あるいは防衛関係では、きまり言葉がある。われわれが今話しているのは"軍事情報"とか"軍事安全保障"とか"安全な電算機設備"などである。軍事機密情報の利用、又は、機密漏洩には、共通したルールがあるが、その点に関しては、ここでは、詳しくのべることはしない。非軍事部門では、用語は確立されていない。"産業上の保安"という言葉は、特許を取った設計や、企業の情報を守るというようなことから、工場や設備の、実際面での保安までも意味している。われわれの問題点から見ると、この言葉は、あまりにも漠然としている。多くの場合、問題となるのは、"プライバシー"の問題である。

プライベートとプライバシーという言葉は、私的な意味の個人と関連を持っている。しかし、ウエブスターの Third New International Dictionary は、次のような定義を下している。

Private ……ある特定の個人、団体、ある階級に属する人々の利用を目的とした、あるいは、その利用を限定し、一般的には公開されないこと。

Privacy ……孤立、隔絶、あるいは不当な監督、監視を受けないこと。

われわれは、コンピュータの中の情報を特定の人々の利用だけに限定することについて話し合っているのである。われわれは、この情報がだれにでも自由に手に入るようにしたくないと考えている。われわれは、この情報を、権限を持たない人々の目から隔離しておきたいと考えている。したがって、きまり言葉を使うことは適切であると思われる。たとえ、まだ内容のしっかり固定していない新語が出てくるという場合が予想されるとしても。

今日ここで取り上げている問題からは、"安全保障"と"機密の"という言葉は、軍事あるいは防衛上の情報や、立場と関連を持っている。"プライベート"、"プライバシー"という言葉は、類似産業、あるいは、非軍事面

の政府の立場を指す。どちらの場合も、情報を受ける権限を持つ者は"知る要求"、あるいは、"アクセスの権限"を持つ。

今回、われわれは、次のことを行なうつもりである。共同利用コンピュータ・システムについての各自の理解を、同じレベルに持って行くために、このシステムの形態について簡単にのべ、情報が知れたり、漏れたりしやすい点を調べてみよう。ピーターズ氏による次の論文が、マルチ・プログラム・リモート・アクセス・コンピュータ・システムのために考案された。安全確保の装置について説明する。次に、安全と、秘密保持の立場について、類似点と相違点をあげて比較検討してみたい。ピーターソン博士とターン博士による最後の論文は、安全と秘密保護の処置の技術面を論じる。最後に、リアル・タイム・システムで、秘密保護の問題にぶつかったことのある3人の討論予定者が来ており、おのおのが、この問題に対する見解と、問題解決への方法についてのべることになっている。

さて、おしまいに、あなた方に関連のある状況に対する、満足のいく安全装置を考案し、それを実行に移すのは、あなた方自身の仕事となる。

先験的には、システムの弱点がどんなに危険なものかわからないという事がいえる。あるコンピュータ・システムにとっては重大な事がらが、別のシステムには、無用のものであるかも知れない。われわれは、秘密保護に関しての、想定上の弱点や不安から考えられる危険については、先入観を持たないという立場を取りたいと思う。それよりもむしろわれわれは、コンピュータ・システムが安全の点でも、秘密保護の立場からも、権限のない者に情報を漏らす可能性について考えてみるだけにしたい。どれだけ保護の手段を講じる必要があるかとか、どんな明白な安全装置が必要であるかとか、ある特定の弱点がどんなに重大であるかなどの問題は、個々の設備内容に関する討議にまわしたいと思う。

図1は代表的な、コンピュータ共同利用システムの、ハードウエア構成を示している。コンピュータ処理用の、ファイル付き中央処理装置と、スイッチング・センターを経て、離れているユーザーを結ぶための通信網がある。まず第一に、われわれは、このファイルに秘密を要する度合い、軍事機密の度合いの異なる情報が入ることがある、ということに気付く。したがって、

これらのファイルに対するユーザーのアクセスは制限しなければならない。不適当な、あるいは権限のない者のファイルへのアクセスは、不正に情報を漏らす可能性がでてくることになる。確かに、ファイルがそのまま盗まれることも可能である。——きわめて大がかりな情報漏洩というわけである。また、コンピュータそのものを利用して、ファイルを不正にコピーし、そのコピーから権限のない者へ情報が漏らされることもありうる。

中央処理装置は、ハードウェアと、ソフトウェアから成っている。ハードウェアに関する限りでは、境界表示レジスター、記憶保護装置、特殊使用モードなどのような、保護の回路が働かないで、不適当なところに情報を漏らしてしまうかも知れない。多くの種類のハードウェアのミスは、次には、漏洩のもとになるソフトウェアのミスの原因とつながる。処理装置は、ハイ・スピードの電子回路で成り立っているので、電磁気エネルギーを放射する。したがって、情報を盗もうとする、第三者が機密情報を手に入れることが想像される。ソフトウェアのミスは、アクセスの制限、ユーザーの確認、記憶装置内の境界制限というような、保護の機能を不可能にさせ、情報をつなぐ経路をまちがえる原因になる。

中央のコンピュータに密接な関連を持っている人間は3種類ある。すなわち、オペレーター、プログラマー、保守のエンジニアである。秒刻みのシステムの作業を受け持つオペレーターは、正しいモニターを勝手に作ったモニターに置き換えたり、権限のない者に対して特別の"ins"(命令)を持つ不正なモニターに置き換えたりして、情報を漏らすかも知れない。また、オペレーターは、システムの中に組み込まれた、保護用の装置を権限のない者に暴露するかも知れない。巧妙なプログラマーとエンジニアの共謀で、長期間ばれずにすむような方法で、自分達に都合のいいように、機械に"bug"をつけることもできるだろう。(ここでいう"bug"とは、プログラムの中のエラーを指すのではなく、盗聴器(マティーニ・オリーブ型)のコンピュータ用送信器にあたるものである。)機械にbugをつけて、何でもないように見せかけるのはごく簡単なことである。

オペレーターのいらないシステムでは、手をつけやすい。原則としては、マシンが部外者によってもbugをつけられることは想像できる。機械保守の

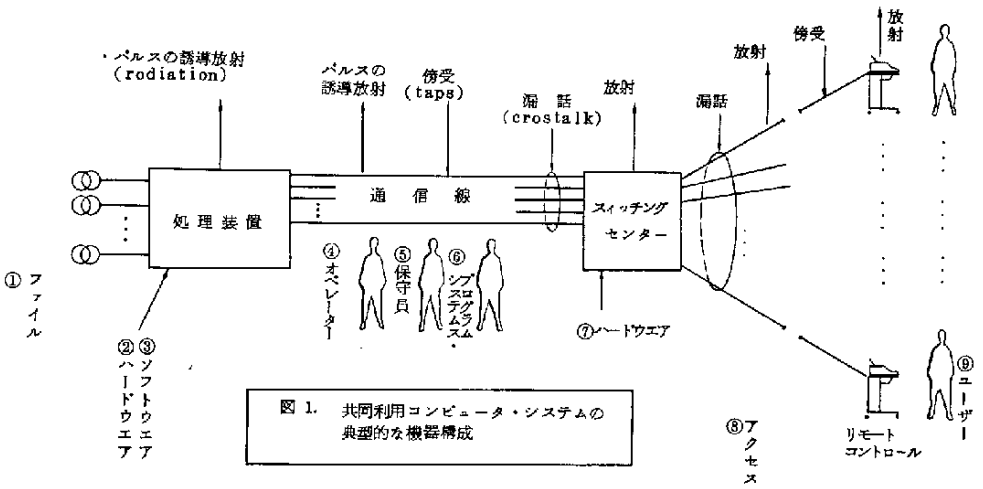


図 1. 共同利用コンピュータ・システムの典型的な機器構成

情報漏洩の原因

① ファイル
- 盗　　難
- コ ピ ー
- 不正なアクセス

② ハードウエア
- 保護回路上の欠陥
- ソフト上の欠陥の一因

③ ソフトウエア
- 保護機能の欠陥

④ オペレーター
- モニターの作りかえ
- 保護装置の暴落

⑤ 保 守 員
- ハード上の保護装置の無力化
- 不正なアクセス

⑥ システムズ・プログラマー
- ソフト上の保護機能の無力化
- 不正命令の用意
- 保護方法の暴露

⑦ ハードウエア
- 通信線連続の失敗
- 混線による漏話

⑧ アクセス
- 付属の記録装置
- 受信機のすえつけ

⑨ ユーザー
- 身分証明
- ソフト上への不正な修正

ほかに
処理装置、通信線などからの誘導放射
傍受、漏話、

過程でも、多少の危険性はある。システムのミスを診断する時、ソフトウェア上の保護措置がどのような符号でできているかを知るための情報が、保守を受け持つ人に、簡単にジェネレートされるだろう。したがって、ある装置を正常に働いているように見せかけて、実際には、保護のための仕組みは素通りしている。というふうにマシンの配線を変えることは、簡単なことであろう。

私が、今、あげたものの、あるものは計画的な行動が必要であるが、あるものは偶然に起きる場合がある。

このように、コンピュータの中央部分では、ファイルへのアクセス・コントロール、ハードウェアからの放射、ハードウェア、ソフトウェア、及びその両方にわたるミス、計画的な侵入行為、システム関係者の事故などに欠陥がある。

中央処理装置からスイッチング・センターおよびスイッチング・センターからリモート・コンソールまでの、通信連結部でも同じような欠陥を持っている。普通の傍受の方法ならどれでも通信線から情報を盗むのに利用できる。通信線の中には、比較的高周波のシグナルを持つのもあるので、電磁放射が、情報をねらう者にとらえられることもある。通信連結部の漏話も、権限を持たない者への情報漏洩をひきおこす。更に、スイッチング・センター自体が、放射や漏話の欠陥を持つこともある。このため、正しい接続が行なわれず、機械が間違ったユーザーにつながることもある。

リモート・コンソールも放射の欠陥を持つことがある。その上種々の記録装置をそのコンソールに接続して、情報を盗聴する可能性もある。印刷装置のリボンを破ってしまうか、刷られたものが判読できないような印字板をデザインすることを考えなくてはならないだろう。

最後には、そのシステムのユーザーがいる。ユーザーとコンピュータの連繋は、スイッチング・センターを経由しているので、中央処理装置は、通話の対象を確認する必要がある。このように、ユーザーを正しく確認する方法が必要であり、その方法を記録装置のとりつけとか、情報の盗聴とか、不正な利用などに対する防止策にしなければならない。ユーザーの確認が完全に行なわれても、特定のファイルと、特定の構成機器に対するアクセスの権利

を証明する問題が残っている。システムに対するユーザーの要求を確認する方法が必要であり、その方法を bug のとりつけ、レコーダー、盗聴、不正利用などの防止策にしなければならない。最後に、ユーザーの中には、ソフトウェアのシステムに巧みに入り込んで、その構造を探知し、オペレーターやシステム・プログラマーにはわからないように、本来入手できない情報に対する " ins "を与えられるように変更しようという巧妙な者もいる。

要約すると、いたるところに人間の手で引き起こされる事故の可能性がある。すなわち、個人の行動が、偶然に、あるいは、計画的に、システムの中の情報の保護手段を侵すことが可能である。ハードウェアの持つ欠陥は、コンピュータ、コミュニケーション・システム、コンソールのそれぞれにある。ソフトウェアも欠陥がある。それから、例えば、システムの仕組みの中にもアクセスの制限、ユーザーの認確、証明などに欠陥がある。これらの点が、どれほど重大であるかは、取り扱かわれている情報の機密性、ユーザーの種類、機械操作関係、ネットワークが組まれる技術、などにかかっている。制限のもっともきびしい場合には、そのネットワークは、すぐ考えられるものの他に、今あげたような侵入行為に対しても防禦がなされなければならない。

この討議は、コンピュータの共同利用システムに対して、情報の不正入手を目的として、偶然にか、あるいは、計画的に入り込もうとする、あらゆる手段を徹底的に考慮したわけではないが、現代のコンピュータ・システムの中の主な欠陥について、そのいくつかを概説しようとしたものである。

この会期中に、次の論文で、これらの欠陥について、更に詳しい検討と、可能な解決法について討議を行なうつもりである。

4. 情報の機密性に関する システムのかかわり合い

カリフォルニア州サンタモニカ；
ザ・ランド・コーポレーション
H・E・ピーターソン，R ターン

序　論

最近のコンピュータのタイムシェアリング技術の進歩は、多くのユーザーに遠く離れた場所にある端末装置で、同時オンライン通信ができるような情報システムを約束する。そのようなシステムに於ては、或るユーザーが保有しているプログラムやデータを、他のユーザーの正当でない通信要求から防禦することの問題が起ってくる。ハードウェアの不完全機能やデバックされていないプログラムに帰せられるような偶発的な接触に対する事前防禦については、既に十分な研究が為されている。機密情報に対して接触しようとする。故意の試みに対する防禦は、最近になって原理的な見地からの検討はされているとはいえ、これまでは断片的な技術上の注意しかはらわれていなかった。この論文は、非軍事的な情報システムに於ける情報の機秘性に対する脅威と適当な対策及び事前の機密防禦の組織的なつながりに関する検討を述べたものである。

この検討は、以下のような情報システムのモデルに基づいている。即ち、一つ或いはそれ以上のプロセッサーを持つ中央処理装置と、それに結合された記憶装置；一連の情報ファイル―そのあるものは固有なものであり、あるものは多くのユーザーによって分けられるものである；地理的に離れた場所にある一連の一般的な、或いは固有の問い合わせ用端末装置；そして民間の通信会社の伝送ネットワークや借用回線或いは自営専用通信線などである。これらのタイムシェアリング・オンライン・システムは、全体的に"システム"と呼ばれる。

＜情報の機密性に対する脅威＞

システムに於ける情報の機密性は、偶然によるものと故意に引き起こされた暴露の両方によって損なわれる。偶発的な暴露の最も一般的な原因は、ハードウェアの破損と、部分的にデバックされたプログラムの使用とである。ハードウェアの信頼性の改善と種々の記憶装置防護プランが、対策として考えられてきた。オンライン・タイムシェアリング・システムに侵入するために熟慮された努力は、消極的なものと積極的なものとの二つに分類されることができる。

消極的な侵入は、システム内のある点で伝達通信の傍受、或いは電磁的な抜き取りによって成し遂げられることができる。伝達通信の防禦へのそうした脅威に対応する十分な努力が、これまでにも向けられてきたとは云え、一般的には、情報の機密性に対する無定見なアプローチは、伝達通信線は安全であると想定している。しかし、実際には　それらはシステムの最弱点なのである。伝達通信網へ侵入するテクニックは、音声会話を聴取することの高度に発達した技術から借用されることができる。（必要とされる最低限の出費は、一揃いの載頭式受聴器（ヘッド・セット）と容量測定器（キャパシター）を手に入れるのに必要な出資よりは高いが、１００弗のテープレコーダーとコード変換テーブルで十分まに合うのだから、なお非常に安いものである。）明らかに、情報の数字的伝達は、例えばモールス符号よりもより高度な機密性を備えてはいない。にもかかわらず、或るユーザーは、電話では伝達しようとしないような価値のある情報を、数字的なシステムに委託しようとしているように見える。

積極的な侵入―ファイル中の情報を直接に手に入れたり、変更したりしようとして、システムに入り込もうとする試み―は、正常な接触手続きを通して、以下のような方法によって、明らかに成し遂げられることができる。即ち；

- 正当と認められない問題（例えば、賃金支給の情報を求めたり、或る一つのデータに個人を結びつけようとすること等）を求めたり、あるいは正当と認められないファイルを“乱読”しようとして、システムの一部に合法的な接触をする。
- 通信傍受や他の方法を通じて、固有な認識を獲得した後で、正当なユーザ

一に"変装"する。

- "知ることが必要"なだけで、情報センターや伝達通信網に関する地位について、システムへの接触を得る(例えば、システム・プログラマーやオペレーター、保守員、あるいは管理職員等)。

あるいはまた、積極的な侵入者は、以下のような方法によって、制御や防禦のプログラムを避けながら、ひそかにシステムへ入り込もうと試みるだろう。

- 非良心的なプログラマーや保守技術者によってつくられた侵入口を利用する。あるいは、多くのシステム制御の変遷を組み合わせて見ると生ずるかも知れない"おとし穴のふた"を探してみつける。(これは、初期のデイジタル・コンピュータの機械語プログラマーに人気ある遊びだった"新しく役に立つ"命令語を探すことに類似している。)
- 以下に述べるような効果のために、伝達通信チャネルを傍受する特殊な端末装置を採用する。
  - ユーザーとプロセッサーとの間の伝達通信を選択傍受することによってシステムの中へ"Piggy back"な侵入をして、それらの伝達通信を変更したり、放散したり、あるいは全く新しいメッセージに取替えたりし、また同時に"間違った"メッセージを送り返したりする。
  - 正当なユーザーが、活動していないのに依然として伝達通信チャネルを保持している時に、"線間"侵入をする。
  - ユーザーの通信終了合い図を抹消して、

    そのユーザーの名で操作を実行する。

多くのこのようなさまざまなことのもとで、正当なユーザーは、固有の接触をするための手続きを整えるのである。

しかしながら、侵入者は正当なユーザーの公認のファイルからは締め出される。

積極的な侵入のためには、安価なテープレコーダー以上のものが必要とされる。何故なら、それには適当な端末装置と伝達通信環への入口が必須だからである。実際のところ、悪意的侵入の試みを始める為には、相当の装備と知識能力が必要である。

情報システムへの侵入の試みが目ざす目標については、可能性のある結果の観点から、多くの権威者による検討がなされてきた。ここでは、我々は、単に、侵入者が着手しようとしている以下のような行為の形態を指摘するにすぎない。即ち、

- ファイルの中の情報がほしい為に、接触を得ようとしたり、あるいは特定のユーザーの情報の関心あるものを発見しようとする。
- ファイル中の情報を変更しようとする（完全なファイルの破壊も含まれる）
- コンピューター使用時間や専用プログラムの自由な使用を獲得しようとする。

ファイルされた情報の性質によれば、侵入の試みは、潜在的な泥棒プログラマーの好奇心を満足させること以上の損害を引き起こすことはないかも知れない。しかし、あるいはまた、それは、例えば"報酬の為のあなたの書類の変更"や産業スパイ活動といった大きな結果に帰着するかも知れない。（情報の機密性に対する脅威の要約としては表1を参照されたい）

より悪意的侵入の筋書きが、侵入の増加への懸賞金として考え出されるかも知れない。情報の機密性に対する脅威は、侵入者ならんとする才知や器用さを見くびることによって軽く考えられたり、取り上げられなかったりすべきではない。

表1　情報の機密性に対する脅威の要約

侵入の性質	方　　法	結　　果
偶発的なもの	コンピュータの不完全機能；ユーザーのエラー；デバッグされていないプログラム	特権ある情報が誤った端末器やプリントアウトでダンプされる。
故意で消極的なもの	通信傍受；電磁的抜き取り；カーボン紙の検査	情報中のユーザーの利点が暴露される；伝達通信の内容が暴露される。
故意で積極的なもの	"乱読"；"変装"；"線間傍受"；"Piggy back"侵入	侵入行為の結果として、特殊な専門的な情報が暴露されたり、変更されたりする

＜対　策＞

前節で検討された脅威の残像は、多くの手法や処理手続きによって打破される。これらのうちの或るものは、元来は、ユーザーがうっかりして互いに他のユーザーのプログラムの邪魔をすることを防ぐためにタイムシェアリング・マルチユーザー・システムに導入され、のちになって、偶発的なあるいは故意に引き起こされた情報暴露を防ぐために発展した。また或るものは、伝達通信網に於ける機密性防禦のための要求にその始まりが見出される。以下に述べる検討では、我々は、さまざまな対策をいくつかの種類にまとめてみた。

接触（アクセス）の管理

この手法は、不当なユーザーがシステムからサービスを得たり、ファイルに接触したりするのを防止することを目指すものである。これに含まれる処理手続きは、公認、識別、証明などである。公認は、システムに加入したり、或るファイルに接触したり、ある種の情報を要求したりする一定のユーザーに対して与えられる。例えば、調査者は、給与支給ファイルから所得統計をまとめることは許されるかも知れないが、俸給と個人氏名を結びつけることは許されないであろう。システムに入り込もうとするユーザーはだれでも、まず最初に、彼自身の身元と所在（即ち、彼が使用する遠隔端末器）を明らかにし、しかるのちに、彼の識別を証明しなければならない。後者は、接触に制限があるファイルが必要とされる場合には、絶対に必要である。これによって、コンピューター経費の誤負担を避けることが考慮される。識別―証明のステップは、何べんも繰返されるかも知れない。（特に、過敏なファイルが必要とされる時には）。

証明することの資格の問題もまた、逆に生じてくるだろう。即ち、処理装置は、適当な方法でユーザーに対する自己の証明を行なう。このことは、彼が侵入者のコンソールと全く交わりがないということをユーザーに納得させるだろう。処理装置からユーザーへの或るメッセージが照合されれば、（例えば、エラー・メッセージや繰返し要求等）それらはPiggy back 侵入者からではなく、処理装置から来たものと証明されるだろう。（もし、種々の特殊な処理手続きがシステムの各分野について必要ならば、それらのしくみ

と効果について詳細な検討が第4節に述べられている）。

取扱い制限

接触を制御する方法は、外部的原因による単純な脅威は除去するが、悪意な努力を止めることは出来ないし、また、不当なユーザーやシステム内部の屓員が"乱読"しようとするのを完全に打破することも出来ない。侵入者は、システム内部でファイル中の情報を抜き取ったり、変更したり、破壊しようと試みるだろう。それ故、過敏な情報のファイルには、何らかの取扱い制限が（標準的なメモリー保護措置に加えて）、課せられる必要がある。例えば、或る移動可能なファイルが、あいまいな処理手続きで扱われることになるかも知れない。そこで、要求のあった時だけなされるデータの変更は、各々のファイルの制御者によって確かなものであることが証明される。全ファイル（もしくは、ファイルの大部分）を複写することは、取扱い制限が課せられる必要のある一再び、ファイル制御者の証明という形で一もう一つの行動である。非常に過敏な情報が取扱われるようなシステムに於いては、"怪しげな"行動をとった場合に特定なユーザーに対して取扱い制限が課せられることが出来る。例えば、非公認のファイルに入り込もうと試みるような何らかのプログラムを全くキャンセルしてしまうことは、"乱読"に対する効果的な対策となるだろう。

脅威の警告

脅威の警告は、即時的反応を備えているような（例えば、仕事の取消しを呼びかけることや処理手順の追跡を始めること等）、或いは事後分析を可能とするようなシステムやファイルに対する現実の侵入やその試みを見つけ出すことに関係がある。脅威の警告は、システムや特別なファイルへ入り込もうとして退けられた全ての試みを記録すること、不法な接触手順を用いること、或るファイルについての異常な行動、防禦されたファイルに書き込みをしようとする試み、ファイル複写のような制限された操作を行なおうとする試み、極度に長い使用期間等々をその範疇に含むだろう。ファイル活動をしているユーザーへの定期的な報告は、可能な乱用や不正をあばき、可能な即時反応と共に、監査を敏速に促進するだろう。そのような報告には、どの頁にも、ユーザー期間中の活動の摘要が、毎月の分析と要約にいたるまで載っ

ているだろう。

機密の交換

機密の変換は、情報を秘す為に、ユーザーと処理装置との間の伝達通信に於けるデータ或いはファイル中のデータを暗号化する方法である。この方法は、悪意の積極的な脅威(" Piggy back " 侵入によって、ユーザーの識別と伝達通信のつながりを分割すること等)に対すると同様に、消極的な脅威(例えば、通信傍受)に対しても向けられることが出来るし、また、非公認の接触や物理的な消失に対して移動可能なファイルの中のデータを防禦することをも可能にする。

機密の変換は、情報レコードの個々の文字或いはそのようなレコードの形態に加える一連の復元可能な操作から成る。復元は、暗号化された形態から元の情報を回復させる(暗号解読)為に必要とされる。機密の変換の種類には以下に述べるようなものがある。

- 置換—メッセージの文字を、一語対一語のやり方で、同一の或いは異なったアルファベット中の文字又は文字群で置き換えること。
  (例えば、英数字の文字を二進数字に置き換える)
- 順序置換—メッセージ中の文字の順序を配列しなおすこと。
- 付加 — ユーザーによって与えられる暗号化用の文字の連続(" 鍵 ")によってメッセージ中の文字を結び合わせるために適当な " 代数 " を使用すること。

いくつかの " 付加的 " 形式の機密変換のうちで、よく知られているのは、メーセージ中の文字を結びつけるのに短かい文字の連続が使用される。" Vigenere 暗号 " と、ユーザーが用意した連続が少なくともメッセージと同じ長さである " Vernamシステム " である。いくつかの変換を組み合わせたような応用が、複雑性を増す為に、使用されるだろう。

一般に、特殊な型の機密変換(即ち、同じアルファベットの中での文字の置き換え)の使用者は、その種類の中でも非常に数多くの変換の選択を有する。(例えば、英語のアルファベット26文字には、26の階乗—4×10^{26}一通りの可能な置き換えの方法が存在する)。特殊な変換の識別となるものは、メッセージを暗号化するためにユーザーによって選択される " 鍵 " であ

る。

どんな侵入者も、当然のことながら、"鍵"を発見しようと試みるだろう。一必要ならば、傍受された暗号メッセージを分析することによって必要とされた努力は、機密変換の"工作の要因"を推測する。工作の要因は、用いられた機密変換の形態や、メッセージ言語の統計的な特徴や鍵の長さのサイズ等できまる。大きな鍵の長さにあまり依り過ぎることに対する警告として、シャノンは次のように指摘している。即ち、26文字で構成された置換記号に使われる鍵を発見するためには、完全な試行錯誤方式による(マイクロセカンド毎に一つの可能な鍵を消去していく)と、平均で約3×10^{12}年が必要であろうと。しかしながら、シャノンによれば、鍵の長さがだいたい等しい数であるような鍵を二組づつに分けていくことを繰返して、各試行毎に一組を消却していく(銅貨の重さの問題と同じこと)には、88回の試行が必要なだけである。

与えられた情報システムに対して決定的であるような工作の要因基準は、勿論、脅威の大きさと情報の価値による。例えば、単独の鍵を破る為には1日中計算を続ける必要があると見積られた工作の要因は、低い水準の脅威に対しては、十分な阻止となるだろう。

機密変換の種類を選択するのに影響するその他の基準は以下のようなことである。

- "鍵"の長さ—"鍵"は貯蔵スペースを必要とするし、防禦されなければならないし、遠隔地へ伝達されなければならないし、システムへ入れられなければならず、その上、記憶されることも必要である。一般に、鍵の長さは短かいものが望ましいように思われるが、メッセージ自体と同じ長さの鍵を用いることによって、よりよい防禦を獲得することが出来る。
- "鍵"のスペースのサイズ—有効な機密変換の異なった種類の数は、試行錯誤的アプローチを思いとどまらせるため、及び、多数のユーザーに対して唯一の"鍵"を指定し、しばしば間をおいて"鍵"を変更することを可能にするためには、出来るだけ多いほうがよい。
- 複雑性—より多くのハードウェアや処理時間を必要とすることによって、機密システム実行のコストに影響する。しかしまた、工作要因の改良もす

るだろう。

- エラーの感度―伝達のエラーや処理装置の不完全機能の結果は、暗号解読を不可能にするだろう。

勿論、もう一つの基準は、実行のコストと処理時間の必要性――部分は、伝達チャネルが含まれているか、或いはシステムのファイルが含まれているかどうかに依る―である。（第Ⅳ節参照）

保全の管理

情報システムに対して機密性を与えることに於いて重要なことは、システムのソフトウェアが明記されたものとして実行する照合である。―これは、プログラムとハードウェアの徹底的な最初の照合及びその後の周期的なチェックを含む。チェックの間、ソフトウェアとハードウェアの修正に完全な管理がなされるべきである。例えば、後者（ハードウェア）は、警告装置が備えつけられて、錠のかかったキャビネットの中にしまっておかれるだろう。各々の修正や修理の後ではハードウェア保全の照合をするのが標準的な処理手順であり、放散する特徴の変化を探知するための検査が定期的になされるべきである。伝達チャネルの保全は、はるかに容易でない問題である。そして、もしも普通の搬送接続器が使われているならば、通信傍受がなされていないことを保証することは極度に困難である。

職員の保全（機密防禦の必須要素）は、この論文の視野の外にあるような根本的な問題を提出する。現実主義の為には、人は全部が全部、信用できるものではないという仮説を立てなければならない。システムの機密性は、可能な限り小数の人員の保全に依るべきである。

＜情報の機密性に関するシステムの情勢＞

先に指摘したように、情報システムのすべてに、同じように情報の機密性の脅威に対して、弱点があるわけではないし、またそれぞれの脅威をうちくだく、異った対策が要求されるだろう。情報処理装置やファイルや端末処理装置のついた情報網の構造と機能は、特に、これらサブシステムの下で、情報の機密性を別々に、個々の検討を保証することである。

情報経路と端末装置

端末装置と情報チャネルが、ユーザから処理装置への主要な連結物であるから、そのシステムの最も弱い部分の情報の機密性が不可欠である。

通信傍受　：　広い地域に拡がったたくさんのユーザは、多くの通信傍受の機会を準備している。物理的に防備された通信回線は高価であるので、このような形での侵入を防ぐのに有効な効果的、実用的な手段はない。その結果、端末装置とプロセサに通用された防禦手段によってのみ、単純な立ち聞きから、特製端末装置への侵入に至る範囲の脅威をうちくだくことができるだろう。積極的脅威に対しては、適当にデザインされた合言葉による認識識別手続が有効であるのに、単なる傍受の脅威に対する防禦も．ごまかしの"ピギーバック"侵入に対する防禦も準備されていない。唯一の広く有効な対策は、機密の変換をすることである。

電磁光線　：　通信傍受の脅威に加えて、端末装置からの電磁光線も考えねばならない。

電磁光線の特徴は、主に端末装置の型によっており、またある場合、一連の保護と電気的侵入の問題をひき起している。秘密の変換の使用は、又、光線の制御の問題も解決するだろう。事実、出来るだけ変換を端末の電子変換装置に接触させることにより、守られねばならない量を小さくし、光線の弱点の範囲をせばめるだろう。

明らかに、これらの問題のむずかしさは、端末装置を入れてある建物や部屋が物理的に安全であるかどうかによるのである。結局、適切に運用することや、タイプライターのリボンやカーボン紙等の処分が大切なのである。

操作方法　：　機密性のあるものと、公のものとを、1つの標準端末装置に結合することが経済的かどうか、まだ決定されていない。しかし、機密のシステムが危くなる可能性は考えねばならないけれども、機密の端末装置を公式の形で運用することは、望ましくなってきているし、また必要でもある。たとえば、どんな目的にも、手でスイッチを入れたりコンピュータにより、機密のハードウェアを容易に避けることができるが、この制御は干渉されやすくなってくる。だから、端末装置の工学は、広範囲にわたったユーザとその機密性の要求に、合理的、物理的、電気的完全さを保障しなければならな

い。

端末装置の識別　：　端末装置の明瞭な確実な識別が、日程や掲示や、制御装置を再出発したり中断してダイアルしなおしたりすることをシステムができるようにすることのために、要求されている。切りかえセンターへの関係の追跡が困難な共同情報線を通して、端末装置がプロセッサへ結びつけられているとき、確実性への要求が主に起ってくる。もし直接配線された連絡網が使われるならば、（通信傍受を除いて）1つの線の中に1つの端末装置があるのだから、確実性も識別も問題でないだろう。

端末装置の識別は、たとえば端末に作成されたユーザ参加の次の2つの部分より成り立つ通信文字を含んでいる。1つは端末装置の種類と名前を含み他の1つは通信文字の最初に特別の端末装置が要求されることを確認する合言葉である。端末装置の確認の他の方法は、コンピューターを使うことである。端末の識別方法が十分に確立された後、プロセッサは端末の秘密のレベルを決定するだろう。すなわち、端末装置に収容できるユーザとか、要求される防禦手段とか。

ユーザの識別　：　端末装置でのユーザの識別は、ユーザの名前や報告番号を確定し、合言葉のリストによって、これを確認することを要求する。もしこの識別手順が十分なら、普通の端末入力装置が使われ、そうでないと、特別の方法が要求されるだろう。たとえばコード化カードを受けとり判断するハードウェアが採用されるかも知れないし、特殊ダイアルボタンが用意されるかも知れない。後の方法は、正しい順序のこれら装置の操作より成り立っている。

その例として、端末装置への物理的な接触がうまく制御されるなら、端末装置の識別がユーザの識別に変わるだろう。（また逆もいえるだろう。）

合言葉　：　明らかに、ユーザや端末装置を識別する合言葉は無限に安全であるとはいえないだろう。事実、通信傍受や通信ピックアップの可能性のある情勢の下では、合言葉はただ1度の使用で危険となる。このような情勢への対策として、確認が必要な度毎に、新しい合言葉をリストからとり出せる"1度だけ使用"のランダム選択合言葉を採用することが提案されてきた。そのようなリストのコピーの一方はプロセッサに保管され、他方は端末装置

に保管されるかユーザに持ち込まれる。ユーザはそれを確認後、リストに次の仕事を加えてプロセッサに伝え、その後消去する。プロセッサは受けとった合言葉をリストと比較し、合致したときのみ処理する。この合言葉のリストは端末装置に特殊な回路で変換されたパンチ紙テープや印刷物で保管される。印刷物は、ただし1つの合言葉によってのみ解読できる安全な保管場所に保管されなければならない。このリストの処理には、特殊なキーが使われる。この合言葉保管方法は、自動読取りができないので、専用入力装置を使用しなければならない。

サイン手続による1度だけの合言葉を準備している防禦は、ユーザの回線に端末装置をとりつけた侵入者による線間侵入に対しては十分でない。ここでは、侵入者は正当なユーザからの情報間システムに侵入できる。このような情勢の下では、1度だけの合言葉の使用は、ユーザからのすべてのメッセージに拡張されなければならない。端末装置による合言葉の自動的作成と包括は、今や円滑な操作に不可欠となっている。そしてプロセッサ中のリストは、プログラムや合言葉作成装置に置きかえられねばならない。

秘密の変換　：　今まで述べてきた識別手続は、傍受や情報網への侵入の脅威に対する防禦対策ができていない。情報網への侵入者は簡単に、情報―合言葉等すべて―を妨害し、情報を変え、自分の指示を挿入する。（たとえば、ユーザに間違った指示を与えるとかして。）しかし、各メッセージの確認のみが“ピギーバック”侵入者が正当なユーザからのメッセージをキャンセルした後のシステムを使うことを予防することができる。

直接回線は、通信傍受に対して安全であると考えられるが、共通回線が安全であることはほとんど不可能である。だから、秘密の変換が正しいキーの所有者にしかわからないコード化したメッセージを表わすようデザインされるので、傍受に対する唯一の効果的な対策は秘密の変換である。だから侵入者にとっては、そのキーを発見することが不可欠のこととなる。コード化されたわかりにくいメッセージを解明する努力が（キーを盗んだり買ったりするよりも）秘密変換の要因である。これは侵入者の才能と知識によると同時に、変換の型にもよる。

特殊な情報網や端末装置に適した秘密変換の型は、情報網の電気的性質や文字の制限や言語やデータの数や端末装置の技術的見地や価格などによって決まる。たとえば、雑音のある情報装置は、自動キー変換（メッセージ自身がキーとなっているような）を使えない。とりかえにより統計的に明らかとなり、規則性をたやすく発見できるだろうから、高度に構成された質問言語は、直接とりかえにくい。情報網や端末装置やプロセッサを制御するために、質問言語が予約されたところでは、制限文字の効果が明らかとなってきている。（たとえば"通信終了"、"転送せよ"とかその他の制御文字）秘密変換は大きな制限があるから、これらの文字が、はっきりと適所に挿入されるべきである。

これらの他に、秘密変換の使用のたくさんの意義が起ってきた。たとえば、端末装置の秘密操作により、システムは、端から端へ（端末装置からプロセッサへ）の秘密変換を準備して、ユーザの秘密要求に応えられる。もしユーザがこれを受け入れないなら、もっと協力して、自分のキーを使って代わりの秘密変換を紹介してやればよい。もしこのことが端末装置に準備できるなら、別の秘密変換回路が準備できるだろう。

他の可能で必要な面は、ユーザに秘密変換を用いるかどうかを専用の報告で指定してもらえることである。これは情報システムの操作プログラムに準備された"秘密指令"の一面である。端末装置から、特にはじめて受けたときは、秘密から公の形に変える度毎に確認すべきである。

ファイル

上述の秘密防禦技術や外部端末装置への制御技術や情報網は、不当な方法による秘密の脅威を少くしてきているのに、(1)非公認ファイルから読みあさる正当なユーザ、(2)操作員や保守員に接触すること、(3)侵入者が物理的にファイルをとり出すこと、等に対して防備されていない。

情報の秘密をファイルに準備するという基本的姿勢はユーザの全秘密に対する権利である ——情報センターの管理者でさえ接触することができないように——。 その上、ファイルに、ちがったレベルの秘密を確保することもできる。このことはすなわち、一方では他の者はこれらのファイルの一部にさえ接触できないのに、ユーザのグループは、会社のファイル全体に接触す

る機会をもっているということである。

これに関して、非公認の目的のために、自己判断でファイルのコピーを用意し保存することは容易であるから、ファイルコピーのような標準ファイル操作は、もし制御されないなら、不適当にみえるだろう。同様にファイルへの書き込みは十分制御されるべきである。たとえば、あるファイルに追加や削除をすることは十分な確認の後に行なわれなければならない。物理的には書けない回路でファイル操作することさえ望ましいかも知れない。

接触制御　：　最も簡単な、最初にサインするという確認識別手続が確立しているところでは、ファイルの制御においては、正当なユーザのリストを保守することに基礎をおいている。もしそれ以上の保守が、特殊ファイルに要求されるなら、ユーザ識別のために、他の合言葉か、特別のファイル処理用合言葉が要求される。ファイル処理用合言葉は、個別の公認ユーザのリストの中か、１つのリストの中に保管される。もし後者（１つのリスト）ならば、システムは、ユーザにリストの中の特殊なところに合言葉を求める。（たとえば１０番目の合言葉）ただ１つのリストは、保管箱も必要としないけれど、本来安全ではない。ファイルの保護はこのように、最初にサインすると同様、認識と識別の要求をくり返し使うことに基づいている。しかしこの防禦方法は、情報網に秘密変換が使われていないシステム（たとえば通信傍受がまだ可能なような）の中では不適当である。

物理的弱点　：　加えて、ファイルへの物理的接触の可能性による脅威の問題が起ってきている。特に補助ファイル（決定的失敗からの救済のための精密なファイルのコピー）がこの問題にかかわってくる。これらのファイルの保管、輸送、準備はすべて、コピーや盗みやオフライン印刷等による弱点をもっている。明らかに、たとえば１巻のテープをもっていることは、妨害者に、ひまな時に情報を熟読する機会を与えてしまう。適用できる対策は、注意深い保管と輸送と物理的にファイルを完全にするシステムと、秘密変換を使うことである。

秘密変換　：　端末装置や情報網には、通常の制御法や物理的防禦手段の失敗に対してファイルの保護がなされるべきである。しかしながらファイルの変換技術はかなりちがった形をとっている。

◎ ファイルの活用レベルもレコードの長さもかなり大きい。

◎ 多くのユーザが1つのファイルを分割できる。

◎ ファイルの操作エラーは、情報網のエラーよりも発見されやすく、制御しやすいし、正されないエラー率は低い。

◎ ファイルのための操作が有効であればある程、ごまかすための秘密変換が多く使われる。

◎ 多くのファイルは比較的完全で、十分大きいので、たびたびのキーの変換は、たくさんの処理に非実用的である。だから高度の要因について秘密の変換が使われるだろうし、キーはそんなには変えられない。

こういう理由で、ユーザからプロセッサへの情報に十分な秘密変換は、ファイルの保護のためには受け入れがたい。

情報ファイルの秘密変換の選択は、主にファイルの量や情報を要求する度合いやファイルの大きさと構成（たとえば短かいレコードで大量の登録）や、ファイル中のデータの構成やユーザの数とかいったものに依存する。これらの要因は、ファイル間でちがっているので、秘密システムには適当なパラメータを考慮しなければならない。たとえば、ファイルの中間より入ることはできないので、ファイル全体を組み入れる連続キーは実用的でない。プログラムによる直接実行が、不合理に処理時間を増大させるので、もし復合変換が望まれるなら、更に平行処理できるハードウェアが要求されるだろう。必要な制御や変換組織の完成のために、そして要求される時間に処理を合わせるために、共通の入出力装置に合う簡単な安全につくられたプロセッサが使われるだろう。

プロセッサ

プロセッサとその連結されたランダムアクセス記憶装置は、基本モニタプログラムと、様々な目的のために作られたシステムプログラムと、広くサービスされたユーザプログラムとデータを含んでいる。モニタの役割は、入出力ファイル処理やユーザの計画や、秘密保護等の基本プログラムをすべて完全に制御してゆくことにより、ソフトウェアシステムを侵入者から守る主ラインを準備しておくことである。

システムエラーや、回復時間のような不慮の事故のときに、システムの一

部分の開始から終了までの間にシステムプログラムのディバッグも可能である。明らかに、そのような完全なモニターは困難な問題である。ピーターは、ソフトウェアによる安全獲得のためのたくさんの原則を述べている。

侵入者は様々の対策をよけて、モニタやシステムプログラムに対して、その制御を弱め、その安全目的を悪くするよう試みている。そのような侵入がプロセッサ施設の外部からうまく試みられることはあまりないので、防禦は、主に、十分物理的な完全さや、職員に依存する。第1歩は、物理的にのみ変えられる厳重にかぎのかかった家に収容された、読むだけの保管物にモニタを保管することである。事実、モニタをモニタ制御の下でのみ操作できるような基本的なプロセッサのハードウェア理論の中にあてはめることが望ましい。

ソフトウェアの完全操作は、定期的に、また修正の度毎に、注意深くチェックされたマスターと一連のシステムプログラムを比較することにより保守されるべきであるし、チームオペレーションによって支えられるにちがいない。（数人の共同作業の形成は、1人のオペレーターやプログラマーが、忠実さを棄てるのより、むずかしさを増す）

完全な管理手法は、秘密保護のプログラムに必要な制御方法や合言葉やキーや決められたリストを挿入するためのディバイスやあるいは保守のために、増強されなければならない。これらのことは、情報センターの職員（すなわちシステムプログラマーやセンターの秘密管理者）たちを確認することを要求するだろう。

秘密保護体系　：　秘密保護は、トップシステム管理者によるシステム操作の体系と、秘密保護プログラムを要求する。この体系の下では、個々のユーザの独立した秘密保護プログラム体系がたくさん存在するだろう。特別のレベルで、この体系に入ることを認められた人が、自動的に低いレベルの体系に入ることは必要ではないし、望ましくもない。システム体系に入るということは、知る必要性が確かめられたときにのみ、許されるべきである。

タイムシェアリング　：　情報システムの完成された様々な型は、プロセッサの情報の秘密に影響を与えるだろう。特に瞬時の保護体系の動的な部分に残りの情報をコピーすることはあり得る。うまく処理された後、きれいに

消去することは、はなはだしく時間を要するので、その解決法は、秘密の情報の見出しとしてプログラムしたり、秘密情報のための一部コアをとり消したりすることである。そして、すぐにそれら見出しや、ページのためのエリアを増すことである。秘密のエリアやページは交換操作の部分として消されるべきである。たとえば、もしプログラム化された数によって適用されるなら、秘密変換は、各分割時間帯のかなりを要求される。だからモニタのハード変換をとり入れることにより、あるいは接触制御や秘密変換操作の別々の平行プロセッサの使用により、秘密変換のハード変換使用が必要となってくる。

ハードウェア事故　：　安全管理について、ハードウェアの完全さという最初の装置制作者の責任の問題がある。すなわち、それが制御されていないあるいは普通に保守されたシステムでさえうまくいかないことがあるという意味で、ハードウェアの事故は決定的ではない。ハードウェアの危険箇所を起完全にするか、あるいはそのシステムの完全さが退化するのに対処することができるかどうかはこれからの問題である。

終り に

タイムシェアリングシステムにおける情報の機密性に関する脅威は確かなことであり、地道な努力のみが、低レベルの侵入努力に対処できる。しかし情報センターの職員の完全さと資格を妥協しないことにより、不合理な経費を使うことなしに、脅威をうちくだくことができるようになった。十分に信頼できる操作員は、次第に、防禦手段を使って、ハードウェアやソフトウェアの保守完備の完成を確立してゆくだろう。様々の脅威に対するこれらの手段の効果の単純な評価は、議題にのぼっている。

秘密は、有効な秘密技術が、処理時間のために、大きな結合度化で、全ユーザに自動的に適用される"消極的秘密"の完成から、ユーザ個人が望むレベルで詳述できる　"オプショナルな秘密"に達するだろう。"オプショナルな秘密の体系は、秘密が、本来ユーザが要求する防禦について課せられるから、もっと望ましいものになってきている。たとえば簡単な合言葉が、十分な防禦手段であると感じるユーザは、その方法により、処理時間とメモリースペースをできるだけ節約して完成することができる。

"オプショナルな秘密"の完成は、プログラミングシステムのことばによって準備された"秘密指令"に基づいているはずである。それらの適当な実施(そして共通の合言葉リストとそのキーの安全保持)はシステムを保証する。それらを使う価格は自から計算時に高率に反映する。たとえば「AUTHENTICATE,K,M」という命令は、すでに、システム中の合言葉の中からこのユーザに割り当てられた"K"というリストから、次の合言葉を要求している。今、操作プログラムは、そのリスト"K"のコピーから、正しい合言葉を受けとり、ユーザとプロセッサに送る。もし受けとったものが、プロセッサの合言葉とちがっていたら、プログラムは、間違いのレコードを"M"すなわち、"Log A"の計算をして確かめる「WRITE LOG A」命令の位置へ転送する。その先の命令は、プロセッサの位置にすぐに警報を発するように作成されている。(あるいは、ユーザの端末装置にも)あるいはプログラムを終了させる等になっているにちがいない。他の命令は、秘密変換やプロセス制御等に適用されるだろう。もちろん、秘密保護は個々のユーザがプログラムにデザインし秘密保護計画を完成させていくことにより、どんなシステムにも準備できるだろう。たとえば、ユーザはその目的のために、システムに準備された命令を増して確実に要求をプログラムするだろう。また、情報網の中に、秘密変換を適用するための計画をするだろう。これらの付加保護計画は、ソフトウェアを完成させるだろうから、外部安全レベルを準備しないで、かなりの処理時間を要するだろう。

その他の仕事 : この文章は、情報の機密性に関する脅威の範囲を探ってきた。そして可能な対策の一連のシステムをとり上げてきた。いくつかのシステムが、すでに固定的に進んでいるけれども、かなりの仕事が、なお可能性を実現へ移行する必要性をもっている。秘密変換を経済的に実行するに当って、特別の注意がはらわれなければならない。すなわち、変換の適用クラスの決定、仕事の要因の確立、コード化したり変換するための経済的ディバイスのデザイン、秘密変換の"疑問言語"の効果を考えること、処理時や要求箇所の決定等である。

過敏な情報ファイルによる大きな情報システムが、すでに実現しつつある。コンピュータ会社は、秘密への脅威や十分な対策を考えることなしには、シ

ステムがデザインされていないということをユーザに保証する義務をもっている。要求と可能な解決策の間の経済的バランスを保証するために、ユーザはこれらのことを考慮に入れるようにしなければならない。これらのことは、過去においてもなされてきた。（たとえば産業設備保護、企業機密文章等）しかし情報に接近する技術は微妙に変化している。同じ技術が、防禦のために準備されるが、我々は、どのレベルの防禦がユーザによって要求されているかを知らなければならない。

参　考　文　献

1) コンピュータと秘密の創作

Hearing Before a Subcommittee on Government Operation House of Reprcsentatives July 26－28 1966

U S Government Printing Office Washington DC 1966

2) P.BARAN

情報とコンピュータと人々

AFIPS Conference Proceeding Fall Joint Computer Conference Part 2 Vol 27 1965

3) S.ROTHMAN

中央政府の情報システムと大統領諮問委員会の秘密報告

September 22 1966

4) E.E.DAVID RMFANO

接触しやすい計算の社会的意義についての考察

AFIPS Conference Proceeding Fall Joint Computer Conference Part 1 Vol. 27 pp 243－251 1965

5) S.D.PURSGLOVE

傍受者：R＆Dから生じた

Electronic Design Vol. 14 No 15 pp 35－43 June 21 1966

6) S.DASH RF SCHWARTZ REKNOWLTON

傍受者

Rutgers University Press New Brunswick New Jersey 19

7) W.H.WARE
安全性と秘密性：類似性と相異性
SJCC 67 Atlantic City New Jersey に提供された
8) R.C.DALEY P G NEUMANN
2次保存のための一般目的ファイルシステム
AFIPS Conference Proceeding Fall Joint Computer Conference Part 1 Vol. 27 pp 213 1965
9) マルチプログラムされたコンピュータシステムにおける安全な思考
SJCC 67 Atlantic City New Jersey に提供
10) P.BARAN
分類伝達：K 安全、秘密、全くの自由思考
RM-3765-PR The RAND Corporation Santa Monica California August 1964
11) C.E.SHANNON
秘密システムの伝達原則
Bell System Technical Journal Vol. 28 No. 4 pp 656～715 October 1949
12) R.L.DENNIS
コンピュータ情勢の安全性
SP2440/000/01 System Development Corporation August 18 1966
13) D.J.DANTINE
情報管理システムのためのユーザの伝達要求
AFIPS Conference Proceeding Fall Joint Computer Conference Vol. 29 pp 403～411 1966
14) R.L.PATRICK 秘密伝達

表　　Ⅱ

情報の秘密に関する脅威への対策 概要

対策 / 脅威	接触制御（合言葉・識別認識）	処理の制限（記憶量・防禦）権力操作	機密の変換	脅威の警告（検査・日程）	完全管理（ハードウェア・ソフトウェア・職員）
偶発的なものユーザのエラー	正しい合言葉を作成しないならよい防禦	過敏性を弱める	合言葉に頼らないなら制御できない。頼るならよい防禦	事故を起しがちと診断し、知識を準備する	適用できない
システムのエラー	エラーに対する義務をよけないならよい防禦	同　上	情報システムの切りかえの場合にはよい防禦	同　上	事故の可能性を小さくする
故意で消極的電磁気	な　し	な　し	過敏性を弱める防禦量を小さくする	な　し	過敏性を弱める
通信傍受	な　し	な　し	同　上	な　し	情報網に適用すれば敏感に応じる
くずかご	な　し	な　し	な　し	な　し	適当な処置
故意で積極的乱脈	必要とみせかける	必要とされる情報を得にくくする	よい防禦方法	成功しないと認識させる。すぐ警告する。	他の対策をみつける
変そう	合言葉を確認する	同　上	合言葉以外の防禦はない	同　上	変そう者が情報を得にくくする
線間侵入	メッセージを使わないなら防禦はない	ユーザの分野に他人を入れない	秘密変換を必要以上にかえない	行動の分析が損失の可能性の知識を用意する	情報網を完成する
"ピギーバック"侵入	プロセッサとユーザの間でくり返し確認しないなら救いようがない	同　上	同　上	警告できる	情報網の確認が助けとなる
システム職員の侵入	変そうすべき	必要とされる情報を得にくくする	この要因は合言葉に頼らなければ、変そうで成功する	同　上	秘密保護システムへの入口のキー
"落し穴の入口"	な　し	おそらくなし	キーへの接触が得られないなら要因となる	同　上	最初の確認による防禦とその後のハードウェア・ソフトウェア確認の保守
残っている情報をダンプする	な　し	交換時に秘密のコアを消去する	コード化された処理が可能でなければ防禦できない	同　上	適用できない
移動できるファイルの物理的獲得	適用できない	適用できない	キーへの接触が得られないなら要因となる	職員の移動の検査	物理的対抗手段とディバイス

参　考　資　料

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

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

(2) 秘密保全規程 ― コンピュータシステム㈱

3. 契約書の例

(1) 事務代行契約書

(2) 契　約　書

1. 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　宗教若くは禱祀の職に至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。

2　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、他に漏らし、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ー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

管理責人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ない。

（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、前条にもとづ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。

昭和44年6月発行

発行所　財団法人　日本情報処理開発センター
東京都港区芝公園2号地1番5
機械振興会館内
Tel（434）8211（代表）

印刷所　株式会社　泰生社
東京都豊島区池袋2－1065
Tel（984）5321（代表）