コンピュータ犯罪と法制度

——情報の不正入手について——

（情報セキュリティと法制度調査研究委員会レポート）

昭和63年3月

財団法人　日本情報処理開発協会

この資料は，日本自転車振興会から競輪収益の一部である機械工業振興資金の補助を受けて昭和６２年度に実施した「情報化と法制度に関する調査研究」の一環としてとりまとめたものであります。

コンピュータ犯罪と法制度

「情報セキュリティと法制度調査研究委員会」 名簿

氏名	所属	役職
委員長 宮澤浩一	慶応義塾大学　法学部	教授
委員 渥美東洋	中央大学　法学部	教授
〃 池上幸弘	富士通㈱　システム本部 第5公共システム統括部第1公共システム部	部長
〃 大谷実	同志社大学　法学部	教授
〃 小泉耕一郎	㈱オリエントファイナンス 電算本部応用開発部	教授
〃 今野衛司	日本ＩＢＭ㈱　技術渉外担当	部長
〃 曽根威彦	早稲田大学　法学部	教授
〃 土屋守之助	日本電信電話㈱　総務部法務室	室長
〃 中森喜彦	京都大学　法学部	教授
〃 中山信弘	東京大学　法学部	教授
〃 西田典之	東京大学　法学部	教授
〃 別府正夫	㈶中小企業調査会	顧問
〃 堀部政男	一橋大学　法学部	教授
〃 三木茂	三木法律事務所	弁護士
〃 三和俱侑	富士銀行　システム開発室	室長
〃 安富潔	慶応義塾大学　法学部	助教授
〃 中山隆夫	㈶日本情報処理開発協会	常務理事

目　　次

第1部　コンピュータにおける情報の不正入手に関する考察 …… 1

1. 現行の刑法，特別刑法等による対処の可能性及び限界 …… 1

1.1 コンピュータ犯罪 …… 1

1.2 情報犯罪とコンピュータ情報の不正入手 …… 1

1.3 財産権保護の観点 …… 3

1.4 通信の秘密保護の観点 …… 5

1.5 一般の秘密保護の観点 …… 6

1.6 処罰の間隙 …… 7

1.7 立法的手当とその問題点 …… 8

2. コンピュータにおける情報不正入手の脅威とその対策 …… 9

2.1 コンピュータにおける情報 …… 9

2.2 ハッカーの跳梁 …… 9

2.3 ハッカー予備軍 …… 10

2.4 システム側の防御 …… 12

2.5 パスワードの漏洩 …… 15

2.6 システム側の更なる防衛 …… 17

2.7 過剰防衛の問題点 …… 18

2.8 システム防御対策の限界 …… 18

2.9 望まれる法制度の整備 …… 19

2.10 国際協力 …… 19

3. コンピュータ・セキュリティと
コンピュータ犯罪に対する法制化 …… 20

3.1 「システム」としてのコンピュータ …… 20

3.2 コンピュータ犯罪と対策 …… 24

3.3 法制化への所見 …… 32

4. セキュリティ・システムの限界について …… 35

4.1 はじめに …… 35

4.2 セキュリティ・システムのあるべき基準 …… 35

4.3　能率性・経済性と安全性について …… 36
4.4　セキュリティ・システムでの
　　犯罪抑止が難しいと考えられる事象 …… 37
4.5　セキュリティ・システムの限界 …… 41
4.6　今後の刑法化にむけて …… 42
5.　通信システムにおける不正行為の脅威とその対策 …… 43
5.1　はじめに …… 43
5.2　不正行為への脅威 …… 43
5.3　不正行為の防止策とその限界 …… 45
5.4　不正行為の態様と法的評価 …… 46
5.5　いくつかの問題 …… 47
6.　テレコミュニケーション・システムと結合した
　　コンピュータに蓄積された情報・資料の保護 …… 50
6.1　はじめに …… 50
6.2　通信秘密の保護とプライヴァシィー保護のずれ …… 52
6.3　「事業者の取扱中に係る通信」の意味 …… 53
6.4　通信事業者以外の者が通信システムに結合した
　　コンピュータ・システムの保護の必要性 …… 55
6.5　結びに代えて …… 57

第2部　情報犯罪の脅威とセキュリティ対策等に関する調査 …… 61
1.　調査の概要 …… 61
2.　層別集計表 …… 77
付録　日本におけるコンピュータ犯罪の事例 …… 105

第１部　コンピュータにおける情報の不正入手に関する考察

第1部　コンピュータにおける情報の不正入手に関する考察

1.　現行の刑法，特別刑法等による対処の可能性及び限界

早稲田大学　曽根威彦

1.1　コンピュータ犯罪

本稿のテーマは，コンピュータ犯罪と情報犯罪とが交錯するところに存在するものである。

まず，コンピュータ犯罪は，様々な観点からこれを分類することが可能であるが，コンピュータのデータ処理・保存機能とのかかわり方を基準としてコンピュータ犯罪を整理した場合，①コンピュータ（データ）の不正操作，②コンピュータ情報の不正入手・漏示，③コンピュータ破壊(妨害)，④コンピュータの無権限使用に分けるのが一般である。本稿の考察は，②に対する現行法による対応を中心とするものであるが，ここに「コンピュータ情報」とは，コンピュータ・ソフトウェア，とくにプログラムとデータとを合わせたものをいう。したがって，「コンピュータ情報の不正入手・漏示」というのは，コンピュータによるデータ処理結果，あるいは入力・処理過程にあるデータ，プログラム等を不正に入手・漏示する行為を意味することになる。

1.2　情報犯罪とコンピュータ情報の不正入手

(1)　情報犯罪とは何か，ということについては必ずしも見解の一致があるわけではない。その一つに，これを「コンピュータ・システム，通信システム，両者が結合した情報ネットワーク・システムのセキュリティに危害を及ぼす行為を中心に，情報をめぐる不正行為」と広く捉えたうえ，情報犯罪を，①盗聴など，通信システムに関連するもの，②ＣＤ犯罪，バンキング・システムの悪用による財産利得など，コンピュータ・システムに関連するもの，③データ通信回線を通じてコンピュータのデータを不正入手。改竄するなど，コンピュータ・システムとネットワーク・システムが結合した情報ネットワーク・システムに関連するものの三つに分類する見解が

ある（板倉宏「情報犯罪と刑事法」警察学論集40巻4号110頁以下）。今後，情報ネットワークの普及に伴い，③の情報犯罪がクローズアップされてくることが予想されている。

情報は価値を担った財の一種であるが，同じ財ではあっても，有形の物質とはもとより，無形のエネルギーともその性格を異にしている。物質・エネルギーに比して，情報の財としての特殊性は，例えばコピーが作られることによってそれが窃取されても，本来の所持者の元に犯行前と同じ情報がそのまま残存することにある。情報の「非移転性」と呼ばれるものがこれである。この点から，情報は，同じく無形の財であってもエネルギーとは異なり，管理可能性説によってもなお財産犯の客体である「財物」の中にこれを含めて考えることができないのである。

また，情報は，使用によって減耗せず，むしろその価値が流通とともに増大し得るところにその最大の特徴を有している。情報の「累積効果性」と呼ばれるものがこれである。これは，情報自体は特定人の排他的な占有の元におかれることなく，情報の市場に流通することによってかえって質量とも豊富になっていくことを意味している。もっとも，企業の情報など，原所有者の側からみれば，情報の窃用に際し原資料が手元に残るとしても，他の同業者により当該技術情報が使われることによって，競業財としての情報の価値が半減ないし消滅してしまうという側面があることも否定できない。例えば，重要な財産的価値を有する顧客名簿は，流通部門全般での利用価値が高い分だけ，その窃取・窃用は競業財としての情報の交換価値を奪うものといえよう。

(2) コンピュータ情報と結び付くことによって，情報犯罪の特殊な類型を形成するのがコンピュータ情報の不正入手（コンピュータ・スパイ）である。コンピュータ・スパイにおいては，電子情報処理資料またはコンピュータ・プログラムを通じて営業秘密・企業秘密等を権限なしで取得することが問題となる。そのかなりの部分は被害者の財産侵害に結び付く経済事犯であるが，必ずしもそれに限られるわけではない。コンピュータ情報の不正な取得および利用の事例がすべて考察の対象となる。例えば，企業の顧客名簿やソフトウェア，一般民間の商用データベースに蓄積されたデータのほ

か，信用情報機関や行政機関のデータベースに記録された個人に関するデータ等の入手も問題となる。コンピュータ情報の不正入手は，これをいくつかの観点から分類することができるが，ここでは，行為の態様を基準として類型化を試みることにしよう。

コンピュータ情報の不正入手の具体的方法としては，次のような形態が考えられる。①コンピュータ情報が記録された電磁的記録物を媒体ごと持ち出す，②媒体を一時持ち出しコピーして返還する，③センター内でコンピュータにアクセスして情報をプリント・アウトし，または別の電磁的記録物にコピーする，④右コンピュータの端末機の画面にアウトプットしてこれを撮影またはメモする，⑤通信回線を通じて自己の端末機から情報にアクセスし，プリント・アウトする，⑥データ通信回線から通信中のデータを盗聴する，⑦電波を傍受する，といったようなものがこれである。

いずれの行為についても，今日コンピュータへの貯蔵に伴うデータの濃密化によりデータの不正入手等がきわめて容易なものとなっている。上記の③・④のように，データ媒体の紛失の発覚を防止するため，データ媒体自体を侵害することなく単にデータがコピーされて窃用されることも多く，膨大な量のデータを迅速に処理するために作られたコンピュータは，このコピーをきわめて容易なものとしている。さらに，データ遠隔処理の場合には，長距離回線の接続および盗聴によってデータの伝達システムへの介入が技術的に可能となり（⑥の場合），無線によるデータの転送も常に傍受される危険にさらされるのである（⑦の場合）。

1.3 財産権保護の観点

(1) コンピュータ情報の不正入手に対し，最初に現行法が財産権保護の観点からこれにどのように対応しているかをみてみることにしよう（的場純男「コンピュータ犯罪と刑事法の問題点」ジュリスト846号13頁以下参照）。まず，行為者がデータ・プログラムの記録された電磁的記録物を持ち出した場合（前出①，以下同様）は，行為者がこれを占有していれば横領罪，占有していなければ占有侵害の態様により窃盗罪または詐欺罪が成立する。また，他人のコンピュータにアクセスしたうえ，データ等をプリント・ア

ウトし，または別の電磁的記録物にコピーした場合（③）も，コピー先であるプリント用紙または電磁的記録物が被害者の所有に属していれば，上と同様である。もっとも，電磁的記録物の持ち出しがコピー目的の一時的なものにとどまる場合（②）には，使用窃盗の可罰性との関係で問題が生ずる。

このように，コンピュータ・データの財産的保護については，現行刑法においても，例えば企業の顧客名簿，商用データベースに集積されたデータなどを入手するため，磁気テープを持ち出した場合など，情報を記録している物の持ち出しや移動を伴うものについては，その外形に着目してその物についての窃盗・詐欺あるいは横領として捉えることが可能である。

また，コンピュータの端末機の画面にアウトプットしてこれを撮影ないしメモした場合（④），あるいは通信回線を通じて外部からアクセスしたうえ，自己の端末機を使ってこれらの情報を入手した場合（⑤），さらに，データ等をプリント・アウトし，別の電磁的記録物にコピーした場合(③)であっても，プリント用紙・電磁的記録物が行為者の所有に属するときは，行為者が部内者である場合には，その者の地位いかんにより，財産的損害等の要件を満たすかぎりでその者に背任罪が成立し，部外の関与者にはその共犯が成立することになる。

しかし，端末機を用い，オンライン・システムを利用して，他人のコンピュータからデータを不法に入手するなど，物の移動を伴わない情報自体の不正入手については，それが一定の部内者の行為であって背任に当たる場合のほかは，これを処罰することが困難である。1.2でみたように，情報は「財物」とはいえないから，企業情報やソフトウェアなどは，財産的価値のあるもので財産的取引の対象となるものであっても，それが有体物に化体されていないかぎり，窃盗罪や横領罪の規定を適用することはできない。また，贓物罪についても，その適用範囲については限界がある。なぜなら，データやプログラムが記録された電磁的記録物を持ち出し（①の場合），あるいはデータ等をプリント・アウトしまたは別の電磁的記録物にコピーした場合（②）に窃盗・詐欺・横領罪が成立したとしても，原本たる電磁的記録物自体の窃盗等として構成されるかぎり，贓物たりうるのは当該電磁的記録物自体であってそのコピーではない，と解されるからである。

(2) 無体財産権の保護という観点から現行法が罰則を設けている例がある。著作権法は，1986年に改正され，コンピュータに関し，従来保護の対象になっていたプログラムだけでなく，「情報の選択又は体系的な構成によって創作性を有するデータベース」も保護の対象とされることになった（12条の2）。したがって，客体であるデータ，プログラムが著作物性を有する場合には，当該電磁的記録物を別の電磁的記録物へコピーする行為が著作物の無断作成といえるかぎりで著作権法119条違反の罪が成立することになる。しかし，著作権法の対象となるデータベースは「創作性を有する」ものに限られており，一般の個人情報や企業内経済情報等のファクト・データベースは保護の対象から外れている。

1.4 通信の秘密保護の観点

(1) データ等の不正入手に関し，通信の秘密の保護という観点から罰則を設けている例がある。一般刑法上の罪としては，信書に関して，これを故なく開披する行為を処罰する信書開披罪（133条）がある。しかし，かりに電磁的記録物を文書と解するとしても，「封緘シタ信書」ではないから，コンピュータ・データの不正入手につき信書開披罪を適用する余地はない。

(2) 特別法上の罪としては，まず，電波法が第59条において，特定の相手方に対して行われる無線通信を「傍受してその存在若しくは内容を漏らし，又はこれを窃用」することを禁止し，第109条において，「無線局の取扱中に係る無線通信の秘密を漏らし，又は窃用した者」を罰する旨規定している。電波法は，傍受自体を禁止・処罰することなく，「漏らし，窃用する行為」を禁止・処罰し，しかも処罰されるのは通信の存在や内容のうち「秘密」といえるものに限られている。

これに対し，通信中のデータを盗聴する場合については，電気通信事業法違反の罪が成立する。同法第4条は，「電気通信事業者の取扱中に係る通信の秘密は，侵してはならない」と規定し，同第104条は，そのような秘密を侵す行為一般を処罰する旨規定している。電気通信事業法では，傍受（盗聴）自体も秘密を侵す行為として処罰の対象になる，という解釈もなされているが，刑罰法規上，秘密とは実質秘をいい，通信の秘密とは当

該通信の存在および内容が一般に知られていないもので，一般に知られないことについて合理的理由ないし必要性のあるものをいうとすると（判例・通説），傍受（盗聴）だけで通信の「秘密を侵した」として電気通信事業法4条・10条で処罰できるか，疑問がないわけではない。

なお，有線電気通信法9条・14条は，有線電気通信の秘密の侵害を禁止・処罰し，郵便法77条は，郵便物を正当の事由なく開く等の行為を処罰し，同第80条は，信書の秘密を侵す行為を処罰している。

1.5 一般の秘密保護の観点

秘密を扱う一定の者について，守秘義務違反罪，秘密漏示罪を設けている法令がある。個人情報の流通という観点からすれば，行為主体に着目して職務上個人情報を知りうる特定身分者が個人情報を不法に流通させる行為が処罰の対象となる。

(1) まず，公務員の守秘義務についてみてみると，国家・自治体には膨大な個人データがあるが，データの不正入手との関連で問題になるものとして，例えば，公務員という身分に着目したものとして，国家公務員法第100条・109条12号，地方公務員法第34条・60条2号，自衛隊法第59条・118条1項1号などがあり，公務員が特定の業務を担当する場合の業務上の必要に着目したものとして，出願中の発明・考案・意匠に従事する特許庁の職員に対する特許法第200条などがある（堀部政男「情報化時代のプライバシー保護」ジュリスト707号88頁以下参照）。

なお，上の国家公務員法100条の「秘密」には個人の秘密であるプライバシーが含まれており，これが個人情報の流出防止に役立っていることは事実であるが，秘密とプライバシーとは本来別個の概念であるばかりか，国家公務員法の守秘義務も，その主たる保護の対象は行政上の秘密であって，プライバシーの保護という観点からは，十分なものがあるとはいえない。また，それ以外に一般的なプライバシー保護のための個人データ保護法もないから，コンピュータによって得られた個人情報を漏らしても現行法上処罰されることはない。

(2) 公務員以外の者に対する守秘義務規定もさまざまであるが（堀部。前掲

90頁），例えば，特定の業務に従事する者に対する守秘義務として，秘密漏泄罪を規定した刑法第134条，公認会計士の守秘義務を規定している公認会計士法第27条・52条がある。しかし，刑法134条は秘密漏泄罪の主体を医師・薬剤師等に限定しているから，プログラマ，オペレータ，キーパンチャなどがそのような個人の秘密につながるコンピュータ情報を漏らしても，秘密漏泄罪を構成することはない。なお，コンピュータのプログラムやデータなどの不正入手に関連して，企業秘密の保護が問題となるが，現行法上これを処罰する規定はない。

1.6 処罰の間隙

(1) 以上みてきたように，コンピュータ・データの不正入手について現行法上処罰の間隙が生じているが，その理由は，次の点に求められる（板倉「コンピュータ犯罪と刑事法」ジュリスト707号146頁）。すなわち，現行刑法には情報自体を直接保護する規定はおかれていない。現行法において，秘密情報，プライバシーにかかわる情報，あるいは財産的価値のある情報等，種々の情報について，秘密漏泄罪など一部の例外を除けば，その不正入手行為を一般的に処罰するものがない。また，コンピュータ・データの不正入手行為には，種々の特別法の規定によって処罰することのできるものもあるが，その範囲は限られている。したがって，コンピュータ・システムによる情報を漏らしたり，悪用したり，外部から盗用する行為自体を正面から処罰する現行刑罰法規はないといってもよい。

(2) このように，コンピュータ・システムやソフトウェアを保護する刑罰法規の不備・不在が指摘される一方で，このような動きに警戒の目を向ける見方もないわけではない（荒川雅行「企業秘密保護とコンピュータ犯罪」犯罪と刑罰3号64頁）。すなわち，わが刑法典が例えば秘密を侵す罪なり名誉に対する罪という形で特定の情報に限って保護の対象としているのは，無形的情報のうちで特に刑法によって保護すべきものをわざわざ限定した趣旨に解されるのであって，このような原則を超えて，処罰の間隙があるとしたり，処罰の一般化を図ることは妥当でない，とするものである。また，例えばいわゆる産業スパイについては，これもまったく野放しにさ

れているわけではなく，現行刑法の枠内で一定の行為は，窃盗・横領・背任罪などで処罰されているのであり，部内者の行為に対する共犯の成立も可能であって，その限りで十分に刑事規制の対象になっている，と主張されている。

1.7 立法的手当とその問題点

コンピュータ情報の不正入手の立法的手当の要否およびその範囲については，様々な意見が存在する。また，かりにコンピュータ情報の不正入手について，新たな罰則を設けようとする場合，このような行為をいかなる観点から犯罪として捉えるべきであるか，という困難な問題もある。

立法措置の要否に対する積極的立場は，高度情報化社会のセキュリティ，市民生活の安全を確保するための法体系の整備は今日の最重要課題の一つであり，財産的価値のあるデータやプライバシー・データなどを不正入手したり漏示した場合にこれを処罰するのは，最近のコンピュータ先進国の立法の主流であって，我が国でもそのような立法措置が望まれる，と主張する（板倉・前掲警察学論集40巻4号122—3頁）。

これに対し，データ等の不正入手を処罰化することに慎重な立場は，その問題点を次のように要約している。すなわち，これを「情報の窃用」の問題として捉えたうえ，①そもそも刑罰によって保護すべき「情報」があるかどうか，②かりにそれがあるとして，その構成要件の明確化には難点が多いこと，③「情報の窃用」に関する処罰規定の新設は，形を変えた無限定な秘密保護規定となりかねないこと，というものである（伊賀「コンピュータの普及と刑事法の対応をめぐる諸問題」ジュリスト846号56頁）。

高度情報化社会・コンピュータ社会の到来は，市民生活に多大の利便をもたらしたが，同時に，市民生活に対する国家管理・統制の危険を内在させていることも否定できない。また，一方におけるコンピュータ情報の保護の要請に対しては，他方で，知る権利に基づく情報公開の要請が対立・拮抗していることを忘れてはならないし，コンピュータ情報がデータの主体本人の利益のためにではなく，データの保有者・利用者の利益のためにのみ保護されるようなことがあってはならないであろう。立法化に当って

は細心の注意が望まれる所以である。

2. コンピュータにおける情報不正入手の脅威とその対策

日本IBM㈱　今野　衛司

2.1 コンピュータにおける情報

一昔前のコンピュータは記憶容量も小さかったため，その都度プログラムやデータを持ち込んで給料計算や会計伝票の積算をやっており，作業をしていない時のコンピュータ内部は何にも入っていない状態であった。然し今日，記憶容量が巨大化するにつれ，諸々の情報やデータがデータベースとして構築されコンピュータ・システム内に常駐するようになって来ている。しかもコンピュータの用途が単なる伝票積算の類から経営戦略の立案に使用する等高度化するにつれ，システムに常駐する情報内容も，経営方針・戦略・営業目標値・製品開発計画の詳細等のトレード・シークレットに属する極秘情報やプライバシー上重大な事柄を含む個人情報など他人の目に触れさせてはならない情報や，更には原子炉や発電所の運転制御プログラムやデータ，そして官庁システム内の国家機密情報等剽窃されたり破壊されたりしたら由々しき社会問題に発展しかねない情報がシステムに常駐するようになって来ている。

片やシステムの方は，昔のような隔絶されたスタンドアロン・システムから外部と回線で連結されたオンライン・システムになり，しかも特定の相手とだけ連結される専用回線でなく，公衆回線に連結される場合が増加し，この公衆回線を辿って極秘情報のつまったシステムへ不特定多数の人間が近づき得る極めて危険な環境になって来ているのである。

2.2 ハッカーの跳梁

このような環境に置かれれば，手元の端末器を使って回線を辿り，他所のシステムに入り込んで中に納われている情報を覗き見する不心得者が出ても不思議ではない。事実米国におけるハッカーの跋扈はよく知られている。

わが国では幸いにして今までのところはハッカー事件が頻発して困ると

いう事態には到っていない。然しこれで安心してはいられないのである。何故今までハッカーが割合い少なかったかというと，手元の端末から回線を辿って他所のシステム迄入り込むという芸当はそれ程簡単な事でなく，端末の鍵盤を機関銃のように叩きまくり，コンピュータと自由にメッセージのやりとりをするのに慣れ親しんできた欧英のユーザーは端末相手に色々なことをする事に抵抗はないのだが日本のユーザーの場合は従来端末で自由にコンピュータとやりとりをするという事にはそれ程慣れておらず，いわんやハッカーをやるための変則的なオペレーションなどに挑戦してみようという技術的レベルに達していなかったのではないかと思われる。然し近年のパソコンの普及とＯＡの普及に伴い，ディスプレーと鍵盤を相手に諸々の操作をするのに習熟したユーザーも増えて来ており，技術的にはハッカーたり得る予備軍ができ上りつつある。

2.3　ハッカー予備軍

ハッカー予備軍の生成は前述の通りであるが，これらの予備軍が実際にハッカー行為に及ぶかどうかという問題がある。

これについては警察庁が昭和６１年１２月に公表した「コンピュータ関連の不正行為に関する意識調査結果について」という調査結果報告に興味あるデータが載っている。なお本調査は，企業の情報処理，情報通信関係の部門でシステム・エンジニア，プログラマ等の職種に従事している者及び大学，専門学校等の情報処理，情報通信関係の学科に在籍する学生等3,000人を対象として調査し，1,548人から有効回答を得たものである。

先ずコンピュータ・システムへの侵入，操作の可能性についての調査結果は次の通りで１5.5％が可能であると答えている。

侵入，操作ができる	２３５人	１5.5％
〃　〃はできない	1,２８１人	８4.5％

更に，如何なるシステムに進入可能と考えられるかという問に対する回答は表２－１の通りで公衆データ通信ネットワークの場合では，半数以上の者が「侵入可能」と考えている。

表２－１　侵入可能と考えられるシステム

	人数	%
1　自動列車運行制御システム	14	6.0
2　交通管制システム	15	6.4
3　販売管理システム	45	19.1
4　銀行業務総合オンラインシステム	56	23.4
5　クレジット・システム	46	19.6
6　乗車券販売予約システム	22	9.4
7　個人信用情報照会システム	51	21.7
8　警備システム	23	9.8
9　気象情報処理システム	19	8.1
10 公衆データ通信ネットワーク	139	59.1
11 大学などの教育・研究用システム	94	40.0
12 データベース検索システム	105	44.7
13 そ　の　他	19	8.1

このように，技術的には侵入可能という者が多数いるのであるが，敢えてそれを実行する事についての意識はどうであろうか。同調査報告書によれば，行ってみたいか否かという問に対する回答は表２－２の通りである。他人のファイルを覗き見したり，それを他人に見せたり，自分以外のＩＤやパスワードを用いてコンピュータにアクセスする（つまり自分に許可されている以外の情報に手を出す）ことをやってみたいと思っている人が約半数も居るのである。

表２－３　許されない行為だと思うか（回答者全体）		1 別に構わない	2 場合とて思よさうれ	3 絶対に許されない	4 無回答
A	勤務先（学校）のシステムに入っている他人のファイルの内容をのぞきみる	123	888	487	50
B	勤務先（学校）のシステムに入っている他人のファイルの内容をアウトプットする	114	832	553	49
C	勤務先（学校）のコンピュータルームなどにたまたまあったプログラムリストやフロッピーディスクを持ち帰る	130	493	879	46
D	キャッシュカードやクレジットカードなどの磁気カードの磁気ストライプ部分の内容を解読する	161	350	987	50
E	自分のＩＤや暗証番号を他人に教える	187	706	604	51
F	勤務先（学校）のシステムに入っているデータやプログラムを他人に見せたり渡したりする	139	538	821	50
G	自分以外のＩＤやパスワードを用いてコンピュータにアクセスする	116	645	731	56
H	他人の作ったデータやプログラムなどの内容を勝手に書き換える	101	307	1,089	51
（Ｉ　以下省略）					

2.4　システム側の防御

上述のような状況下において，システム側としてもまったく無為無策でいる訳ではない。当然然るべき防御手段がある。然し，総てのシステムがこの防御手段を装着しているとはかぎらず，中には裸のシステムもあり得る。防御手段として一番普遍的なのは，システム内の情報へのアクセスを制御管理するソフトウェアを組み込む云わば論理鍵機構を装着することである。然し，如何にシステムに防御体制を組み入れても，それを預る人間

表２－２　行ってみたいと思うか（回答者全体）		1 大いに思う	2 思う	3 思わない	4 無回答
A	勤務先（学校）のシステムに入っている他人のファイルの内容をのぞきみる	72	363	1,064	49
B	勤務先（学校）のシステムに入っている他人のファイルの内容をアウトプットする	49	268	1,183	48
C	勤務先（学校）のコンピュータルームなどにたまたまあったプログラムリストやフロッピーディスクを持ち帰る	27	118	1,357	46
D	キャッシュカードやクレジットカードなどの磁気カードの磁気ストライプ部分の内容を解読する	88	291	1,120	49
E	自分のＩＤや暗証番号を他人に教える	25	106	1,364	53
F	勤務先（学校）のシステムに入っているデータやプログラムを他人に見せたり渡したりする	35	156	1,306	51
G	自分以外のＩＤやパスワードを用いてコンピュータにアクセスする	53	247	1,192	56
H	他人の作ったデータやプログラムなどの内容を勝手に書き換える	35	92	1,371	50
（Ｉ　以下省略）					

更に，他人のシステムに侵入して情報を覗き見したりすることについての罪の意識についてはどうだろうか。驚くべきことに，そのようなことは許されないと考える者は１／３しか居らず，大多数はやっても構わないと思っているのである（表２－３　参照）。

が厳重に管理しないと，以下に述べるように防御体制は機能しなくなる。これは，どんなに精巧かつ頑丈な錠前をとりつけても，鍵が他人の手に渡ってしまっては役に立たないのと同じである。

2.4.1 リソース・アクセス・コントロール

システム内の情報資源（リソース）へのアクセス・コントロール機構とは，簡単に云えば，リソースにアクセスする事を許されているユーザーには予め鍵を渡しておき，その鍵を使わなければアクセスを拒否するという機構である。この鍵としては通常ＩＤナンバー（User Identification Number）とパスワードが使われる。具体的には，或るユーザーが端末からシステムにアクセス申し入れをするとシステムはＩＤ番号とパスワードの呈示を求める。それに答えてユーザーはＩＤ番号とパスワードを端末から送り込んでやる。システム側は送られて来たＩＤ番号及びパスワードを，予めアクセスが許されているものとして登録されているＩＤ番号群及びパスワード群と照合し，一致するものがあればパスさせてアクセスを許すし，一致しなければアクセスを拒否するという仕組みである。なおアクセスを許すＩＤ番号・パスワード群は各情報ファイル毎に決めることができる。即ち各ファイル毎に誰と誰がアクセスしてもよいものであるかを定義することができる訳である。つまり，情報の入った抽出しのうち，或るユーザーに与えられた鍵で開く抽出しもあれば，開かない抽出しもあり，どれが開きどれが開かないかは予め任意に設定することができるという訳である。

さて，ＩＤ番号とパスワードの二つが鍵であるように前に述べたが，実はＩＤ番号というのは個々のユーザーのシステム内でのニックネームのようなものであり，電子メールを送る場合などに宛名として使われるものであるため公開されるのが普通（コンピュータ関連の仕事に従事している米国人などは最近よく名刺に電話番号と並べてＩＤ番号を印刷している）であり，本当に鍵の役割を果しているのは実はパスワード丈である。パスワードこそがシステム内の情報にアクセスするための秘密の鍵なのである。そしてシステムは，アクセスを試みてきたユーザーが送ってきたパスワードが正当なパスワードでありさえすれば扉を開いて入れてくれる。そのパスワードを送って来たユーザーがそのパスワードの本来の持主でありアク

セスを許されている当の本人であるかどうか迄は関知しない。これは正しい鍵さえ使えば，金庫の持主本人が使おうと泥棒が使おうと金庫の扉は開いてしまうのと同様である。そして，ここにハッカーの暗躍の道がある。つまり，何等かの方法でパスワードさえ手に入れれば，そのパスワードの本来の持主でなくても，堂々とシステムに侵入できる訳である。

2.5 パスワードの漏洩

以上のような次第であるから，パスワードというものは大変に大切なものであり，それを授与されたユーザーはその番号を自分丈の秘密として守り，決して他に漏洩しないように厳重に管理することが求められるのであるが，往々にして漏洩してしまう場合がある。いくつかの例を挙げてみよう。

(1) 部下に端末操作をやらせる場合

これは偉い人の場合程起り易い。極端な場合，例えば大企業の社長が或るデータを欲し，それがコンピュータ・システムのデータ・ファイルの中にある場合，社長自ら端末を使ってその欲しいデータを取り出すなどということをやるだろうか。恐らく否である。近くに居る端末操作のできる社員に操作の代行を指示することになろう。そしてその際，社長はわざわざ席を立って端末の処まで出向き，自分のパスワードを自分で入力するということをやるであろうか？。これも否である。多分社員にパスワードを書いたメモを渡し，すべての操作を任せるであろうと考えるのが自然ではなかろうか。そしてこの瞬間，社長しか見られない最高機密の扉を開く鍵が，本来それらを見る権限のない一社員の手に渡ってしまった訳である。以降この社員は社長の鍵で開く扉はどれでも，いつでも開けて最高機密を覗き見することができることになる。

(2) パスワードの類推

パスワードは英字，数字８文字以内で作れとするシステムが多い。各ユーザーはこの条件の下で任意のものを考え，自分のパスワードとしてシステムに登録する訳であるが，任意に考えると云っても大概覚えやすいものとして，誕生日だとか，氏名のイニシャルと電話番号だとか……考える

所は似たりよったりであるのが現実の現象であり，ここにハッカーのつけ入る隙がある。即ちハッカーは，生年月日や，電話番号や車の番号やその他の個人情報を調べ上げ，それらを元に考えられそうなパスワードをいくつも試案して，それらの試案したパスワードを次々に使って実際にシステムにアクセスを試み若し正解があればシステムの扉は開いてしまうという試行錯誤でパスワードを探り当てる。

(3) メモの盗難

パスワードは本来記憶に留める丈にして，何かにメモするのは避けるべきものであるが複数のシステムに関わったり，或いはパスワードの漏洩を恐れて日毎にパスワードを更新することを要求されたりすると，次々にいくつものパスワードを覚えなければならなくなり，段々それが不可能になってくる。特に前述の生年月日や車の番号を使いがちなためハッカーによる類推がやり易くなるという危険を避けるため，システムによっては乱数を発生させて，その中から選ばせるという方式をとっている場合もあり，この方式ではハッカーによる類推は困難になるものの，正当なユーザー自身完全にデタラメな数字の羅列をパスワードとして記憶するのも至難の技で，結局メモしてしまうことになる。しかもこのメモは，机の奥深く納いこんでは使用上不便で仕方がないので割合い簡単な処に置くことになり，比較的簡単に他人の目に触れ易いという事情がある。

(4) トラップ

これぞハッカーの本領発揮というパスワード盗みの方法で，要するに，パスワードのパターンで識別してシステムの中からパスワードを見つけ出し，仕掛人に知らせるというパスワード盗みの為のプログラムを作ってそれをコンピュータ・システムにこっそり挿入しておくという方法である。この種のプログラムを仕掛けることを概ね「トラップ」と称している。

(5) 恐　喝

不粋な方法であるが，システム関係者を威して強引にパスワード情報を提供させるという手もある。

2.6　システム側の更なる防衛

上述のような，不正情報入手の試みに対して，システム側は最早打つ手がないのかというとそんなことはない。例へば，(2)の類推に対しては，無効なパスワードを3回送って来たら最早アクセスの試みを拒絶し，当る迄試してみるという試行錯誤を許さないという手もあるし，一応正当なパスワードを送って来てもそのままシステムへの回線を繋がないで，名乗っているユーザーＩＤが予め登録している電話番号の方へ，システム側からかけ直すというコールバック・システムを採ることで危険を回避する手もある。コールバック・システムとは例えて云えば次のような仕組みである。即ち，或る会社の製品開発部へ専務の某であるが今開発中の新製品の発表日と予定価格を知りたいという電話が入ったとする。専務の某と名乗ってはいるが果して本当に本人か否か確信のもてない開発部では，何らかの口実で即答を避け，一旦電話を切って後刻，逆に開発部から専務某の方へ電話を入れる（コールバック）こととした。コールバックしてみたら，当の専務は，私はそんな質問の電話をした覚えはないということであった。最初の電話は専務の名をかたったスパイ電話であったのである。この会社ではコールバックすることにより，スパイ電話の危険を回避し得た訳で，以後この種の電話にはコールバックで応じるよう全社に通達が出された。

これは実際にあった話である。この方式をシステムに採用したのがコールバック・システムである。

或いは，ワイヤートラップ（回線の途中で伝送中の情報を剽窃してしまう）対策として剽窃しても読めないように情報を暗号化してしまうだとか，システム側にも二重三重の防御策があるにはある。

話は少し横道にそれるが，最近はコンピュータ処理による暗号化で，キーなしで解読しようとすると最高速のコンピュータを使っても数千年かかるという風な方法も使われており，実際問題として最近の暗号は解読不可能であると云い切ってもよい。それでは，暗号化しておけば完全に犯罪を阻止できるのかというと，そうはいかない。何故かというと解読せずとも悪用し得るケースが色々あるからである。例えば，ハズレ馬券をアタリ馬券に改竄しようとする試みを阻止するため，馬券の裏面の磁気記録情報を

高度に暗号化しておけば改竄を阻止できるかというとこれがまったく駄目である。磁気記録情報を解読して特定の番号を書き替えてアタリ馬券に改竄しようとすればこの作業は不可能に近く，暗号化の効果はあった訳である。然し，アタリ馬券を１枚持って来て，その磁気記録情報をすべてそっくりそのまゝハズレ馬券の磁気膜上に複写すれば，暗号解読を要せずにアタリ馬券もう一枚のでき上りという訳で，暗号は何の防御にもなりはしないのである。このような例は考えれば他にも色々ありうるのである。

2.7　過剰防衛の問題点

安全性を重視する余り，幾重もの防御機構をとり込んだらどうなるか。確しかに安全性は増すかも知れないがシステムとしては固くて使いづらいものになり得る。又経費も嵩む。例へば，コールバック・システムを採用すれば，いつでも何処からでも回線を通じて中央システムを利用できると云うオンライン・システムの特徴・利点を正当なユーザーも又放棄しなければならなくなる。

世の中には，公衆回線を経由して，どんなシステムにでも侵入してみせると豪語しているハッカーも居ると聞く。このハッカーからシステムを守る方法は本当にないのか？。いたって簡単な方法がある。システムを回線から切り離せばよい。そうすれば，如何に優秀なハッカーたりとも，遠く離れた地点から回線を辿ってシステムに侵入することなど金輪際できっこない訳である。

但し，正規のユーザーの方も，オンラインシステムの利便さを一切諦めなければならなくなる。

2.8　システム防御対策の限界

上で若干述べたように，安全対策は往々にしてシステムの使用上の利便性を制限することになるし，当然経費もかかる。従って，安全対策丈を前面に押出して完璧な防御策を構じる訳には行かないのである。経費・システムの有効性とバランスをとって，どこかで妥協するのが合理的・現実的な解であろう。

とすると，ハッカーによる情報の不正入手の危険が残る訳である。

2.9 望まれる法制度の整備

以上概観したように，情報の不正入手防止策をシステム丈でやるのは，極端な方法をとれば不可能ではないにしろ，現実的ではない。現実的には，安全対策とシステムの利便性，コスト等のバランスを勘案した上で，適度の防御策を構ずることになろう。そして，これでは，ハッカーの危険をなお残したままになる場合もあろう。

片や，2.1～2.3で述べたように，技術的に力のあるハッカー予備軍がすでに少なからず存在し，しかも勝手に他所のファイルを覗き見することが許されることであると意識しているのが半数以上というのは由々しき事態であろう。このような危険な行為を取締れる「法制度」を早急に整備し，先ずこのような行為は「犯罪である」ことを明確にし，若し犯した場合には然るべき懲罰をもって望めるようにし，これを以って，情報の不正入手行為にブレーキをかけられるようになることが切に望まれるのである。コンピュータにおける情報の不正入手・改竄・毀損の如き，重大な影響の波及する危険な行為の阻止には，システム側の防御対策のみならず，法による牽制・教育による意識改造の三者協力で臨む必要がある。

2.10 国際協力

筑波の高エネルギー物理学研究所のコンピュータに侵入したハッカーはドイツ人で，西独からはるばる国際回線を辿ってやって来たものであったらしい。今後国際通信が普遍化するにつれ，国境を越えたハッカーの暗躍の危険はいや増して来る。

とすれば，法制度の整備も国内での事件に対処する丈でなく，日本人が外国の端末から日本のシステムに侵入した場合，或いは外国人が外国の端末から日本のシステムに侵入した場合等の取締りについて国際協力・合意を確立し，グローバルな取締体制を確立することが求められる。

3. コンピュータ・セキュリティとコンピュータ犯罪に対する法制化

富士通㈱　池　上　幸　弘

高度情報化時代を迎えて，その中核を担う「コンピュータ・システム」の役割が加速度的に増大している。既に多くの情報システムの進展が社会・経済構造に様々の変化をもたらし，一個人の生活環境そのものが「コンピュータ・システム」を除いては考えられない世の中である。高度情報化時代においては，「情報」が従来の人，物，金といった資源と同列に，或いはそれらを超えて活用される事になる為に，従来の資源管理の概念では規範し難い諸々の課題を提起する様になってきた。情報自体が価値を生む様になって，社会の中に存在する様々の制度・基準といったものの見直し・改革が必要になっているのもその一現象である。価値ある情報は，その流通，加工，蓄積技術が進歩するに比例して殆ど無限の新しい価値を生み出す事になり，資源としてこれを利用するアプリケーション（応用技術）の研究も又日進月歩である。（表３－１）コンピュータ・セキュリティに代表される新しい制度・基準の検討と一方での急速な技術進歩といういわば追いかけっこが始まっているのだが，本稿では「コンピュータ・システム」がさらされている脅威への対応という課題についてシステムの提供者側の立場から，改めて整理を試みることにした。

3.1　「システム」としてのコンピュータ

良く知られている通りコンピュータは機能的に分化された様々の資源㈱から成るシステムである。コンピュータに対する脅威とは，「システム」に対するそれを意味するものであるが，様々な法制化議論の中でもこれを画一的に定義付ける事の困難さが数多く指摘されている。

コンピュータ・システムの直接的な資源㈱はハードウェア，ソフトウェア，媒体等であり間接的なものとしては，システムを運用する人的資源や様々の設備・建物等がある。（表３－２）守られるべき資源㈱はぼう大な数となるのだが，これらは単体として機能するわけではなく，目的・用途によってシステム化されて利用される事になるので，その組み合せは殆ど

表３－１　情報システムの進展

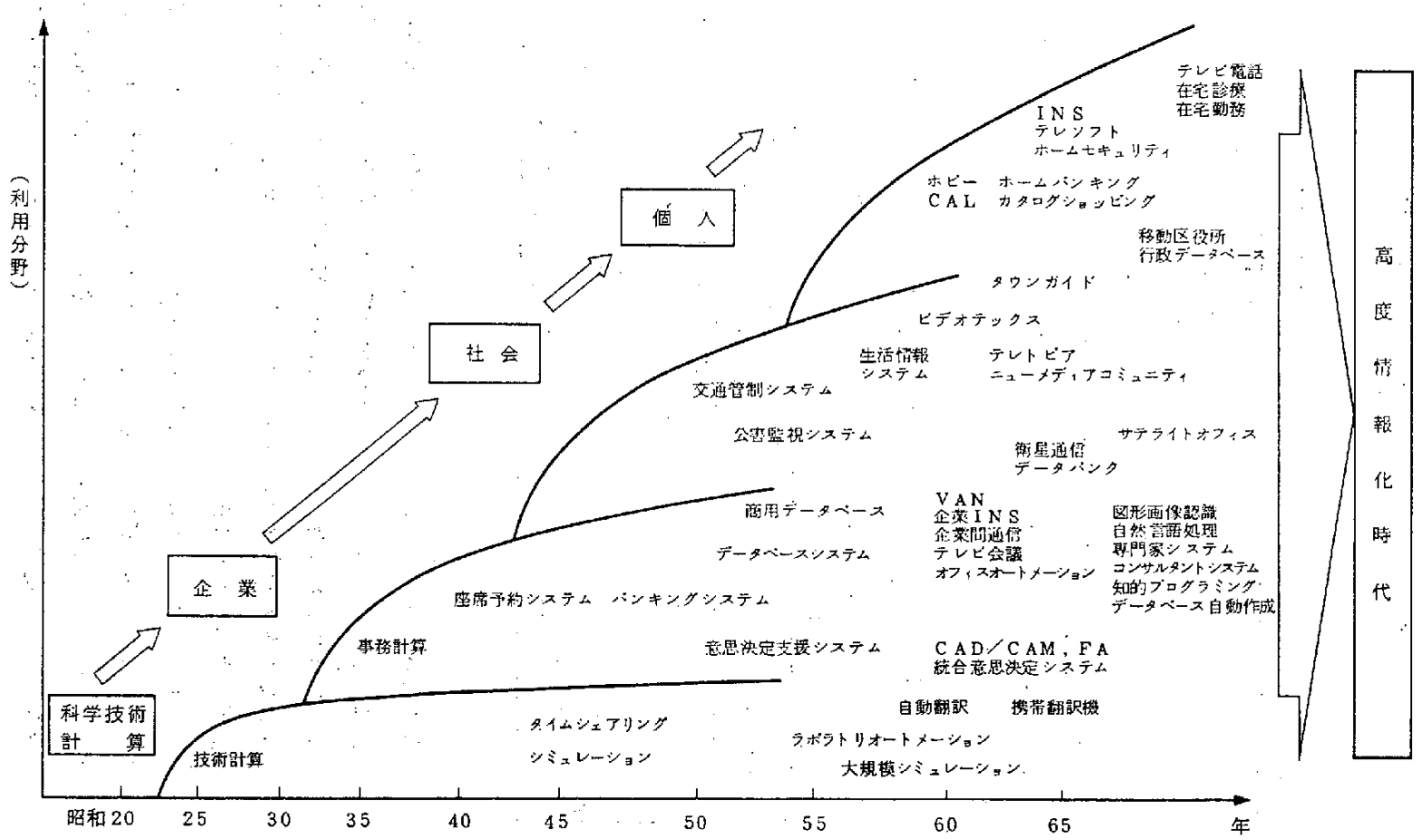


表３－２　コンピュータシステムの構成要素

―コンピュータサービスを実現し，また守られるべき資産―

分類		内容	例
直接的資産	ハードウェア	メーカ提供の各種装置	中央処理装置，主記憶装置，周辺装置，ＣＣＰ，端末装置，パソコン，オフコン，ミニコン
	ソフトウェア	メーカ提供の各種プログラム ユーザ作成の各種プログラム	オペレーティングシステム，サブシステム，ユーザアプリケーション
	ネットワーク	データ伝送のための各種機器	通信回線（特定，公衆，ＤＤＸ），通信機器（モデム，ＬＡＮ，ＣＣＰ，交換機）
	媒体	データやプログラムの格納用	ＤＡＳＤ，ＭＴ，フロッピィ，カートリッジ，紙テープ／紙カード，ＩＤカード，ＩＣカード
	データ	コンピュータ中にあるもの 回線上にあるもの 媒体中のもの	管理ファイル，マスタファイル，ジャーナルファイル，回線データ，端末ファイル，ライブラリファイル
	ドキュメント	システム開発・運営用 業務用	管理資料，仕様書，操作手引書，メーカ提供マニュアル，帳票（伝票，証書，通帳）
間接的資産	人	コンピュータシステム要員 利用者	システム管理者，プランナ，プログラマ，オペレータ，ライブラリアン，エンドユーザ，一般ユーザ
	施設	コンピュータシステム用設備・建物	コンピュータ室，電源設備，空調設備，防災設備，倉庫，金庫，建屋

無限である。昨今の様にシステムが益々大規模・複雑化してくればくる程，それに対するアクセス・ルートや機会が増大し，容易にシステムに侵入できるという皮肉な現象をもたらしている。様々な安全基準も個々のシステム構成要素を対象にキメ細かさを増してはいるが到底システム類型の全てを網羅できるレベルに達しているとはいえないであろう。

コンピュータ・セキュリティとは「コンピュータ・システムを安全な状態に保つ事」であるが具体的な対策の一つに「信頼性対策」がある。システムの信頼度は精度に限界があるものの係数として算出が可能であるので，手段によって実現するシステムの信頼度向上を比較でき，例えば機器の二

重化等の安全対策によって生じる対策効果についても測定可能である。コンピュータ・システムの提供者や運用者にとって対策を講じうる為には，この様な効果測定がなされて初めて具体的なものとして受けとる事が出来るのであって，ハードウェアやソフトウェアの障害（故障），人的誤り等への対応はこの範疇に入る。しかし乍ら犯罪行為を伴う意図的脅威の様にその目的が極めて予測しにくいと同時に，脅威の形態がシステムの規模，内容，機能等によって著しく異なるものである場合には，対策についての効果測定も殆ど不可能であり，具体化が企りにくいのが現状である。

意図的脅威の対象は概ねシステム資源(*)の悪用であり，破壊，不正使用，プライバシーの侵害がこれにあたる。コンピュータ・システムの凡ゆる構成要素がこの脅威にさらされているわけで。それは今後益々増大するであろう「システム」としてのコンピュータのもつ大きな影（脆弱性）に他ならない。（表3－3，表3－4）

表3－3　コンピュータシステムへの脅威

分類	脅威	内容	例		脅威のターゲット
偶発的	災害	コンピュータシステムの外部からの自然現象による障害	地震，火災，風水害，施設不良，落雷，電力異常，動物害，漏水，温湿度異常，電磁気		サービスの妨害
	故障	コンピュータシステムの構成要素自身に発生する障害	ハードウェア障害，ソフトウェア障害，ネットワーク障害，端末障害		
	過失	人の誤りや怠慢が原因となる障害	アプリケーションエラー，オペレーションエラー（機器／媒体取扱い，システム操作），データ入力ミス，施錠ミス，チェックミス		
意図的	故意	人の意図的な悪意に基づく行為による障害	破壊	コンピュータシステムの破壊，施設の爆破，データ・プログラムの破壊・改ざん	
			不正使用	CPU，端末の無断使用，備品の流用媒体，データ・プログラム・ドキュメントの不当使用と持ち出し（データ侵犯）	資産の悪用
			プライバシー侵害	個人データの不当収集，不当使用，不当公開	

表３－４　コンピュータ犯罪の認知状況（昭和46年～60年）

区分＼年次	総数	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
総数（件）	58	1		1	1	3	1		4	3		10	6	6	12	10
不正データの入力	43			1	1	2	1		3	3		6	5	4	8	9
データ，プログラム等の不正入手	9	1							1			1	1	2	2	1
コンピュータの破壊	1					1										
コンピュータの不正使用	4											3			1	
プログラムの改ざん・消去	1														1	

出典：警察白書

3.2　コンピュータ犯罪と対策

3.2.1　ユーザー・メーカーの役割と対策

コンピュータ・システムに対する犯罪の可能性は，実はシステム自体がもっている諸々の側面によってもたらされるが，それらを纏めると以下の通りである。

①　システムにおける大量処理能力

——短時間・小人数での大がかりなデータの改ざん，架空データの挿入等への無防備性

②　データ処理過程及び記録の不可視性

——人的注意力による不正・誤り防止・発見の限界

③　データ及びデータ処理の特定部内集中

——自然的に業務の正否又は適否を検証する効果の希薄性

④　遠隔地よりのデータ・アクセス

——機会，範囲の増大

犯罪予防の為にはこうした側面に適用した効果的な対策が必要であるが，これらはシステムの運用者・利用者側（ユーザー）だけに委ねられるべきものではなく，システムを提供する者（メーカー）にとっても重大な義務である。ユーザー，メーカーが夫々の立場において果す役割はかなり異なったものになろうが，真に効果を発揮する為には両者一体と

なったトータルなアプローチが必要となってくる。（表３－５）

表３－５

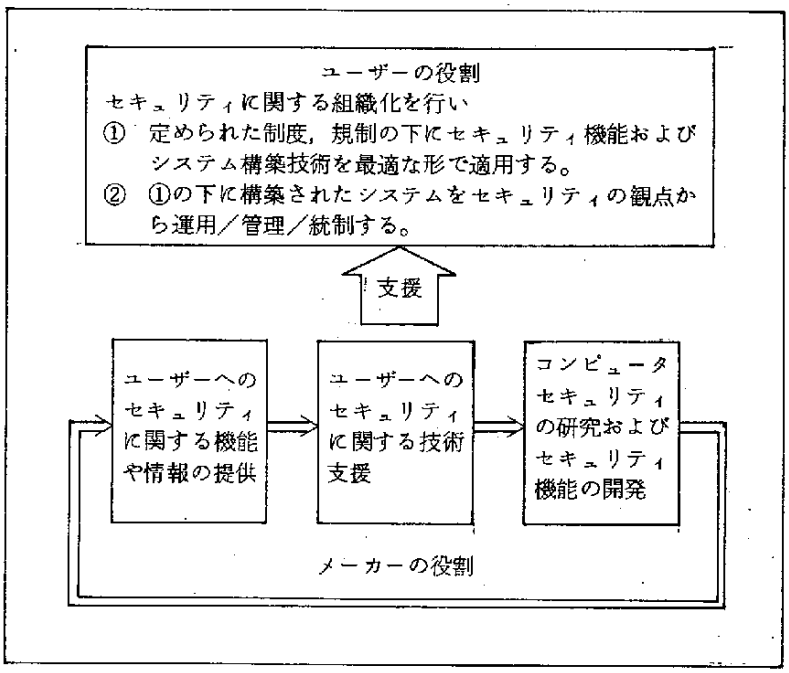


表３－６はこの様な対策の現状において展開されているものの取り纏めである。

表3－6　故意への望ましい安全対策

脅威の内容	望ましい安全対策	セキュリティ機能
故　意 1. 破壊・改ざん (1) コンピュータシステム・設備の破壊 (2) プログラム，データ，ドキュメントの破壊・改ざん 2. 不正使用 (1) ハードウェア ・CPU・端末の無断使用 ・備品の流用 ・媒体の窃盗 (2) ソフトウェア ・プログラムの不正使用（盗み見・複写・盗聴・持出し・窃盗） ・データの不正使用 ・ドキュメントの不正使用 ・プライバシー侵害（個人データの不正収集・不正使用・不正開示）	**1. 入退管理の徹底** (1) コンピュータ室，端末室，データ等保管室などの区域を囲繞し，入室資格者を特定 (2) 上記区域について，厳重な入退館・入退室管理を実施，資格者の確認，記録作成	・入退室管理機能 ・本人確認用カード ・扉の開閉制御 ・入退室の監視記録 ・映像による監視記録
	2. アクセスコントロールの実施 上記入退管理は有効であるが，反面，外部の端末からのアクセスおよび内部利用者の不正アクセスに対しては防御が困難な面がある。このためコンピュータシステムの中で論理的に「アクセスの正当性の確認」をすることが望ましい。 2.1　利用者確認 (1) 端末確認 種別，識別コード，暗証番号（パスワード）による資格確認 (2) 本人確認	・暗証番号（パスワード） ・IDカード（磁気・IC） ・PIN-PAD ・印鑑照合
	情報区分 / 具体的手段 / 考えられる危険 1. 本人のみが知っている情報 / 暗証番号 / 盗み見 2. 本人のみが所持しているものによる情報 / IDカード・（磁気・IC），印鑑 / 盗　用 3. 本人の身体的特徴による情報 / 指紋・声紋・サイン・手形など / － **事　例** 某社による共同オンラインシステムでは端末の電源投入時に，会社，部店コードなどにより正しい接続か否かを自動的にチェックする。またホスト内のソフトウェアに会社別の管理テーブルをもち，加入者以外からのアクセスを監視する。この機能により，たとえ回線工事のミスなどが生じても他社のアクセスを排除する。 (3) 相手確認機能 相手の確認は厳密に行う場合経済的に負担が大きくなる。費用と効果との兼合いであるが，(a)コールバック方式のように一旦端末を切断する方法，（①端末起動，②利用者確認，③回線切断，④ホストからの端末再起動，⑤運用開始），(b)従来の印鑑や署名の役割を電子的に表現するディジタル署名方式などがある。 2.2　利用者のシステム内における行動の確認 利用者とプログラムの対応をチェックし，利用者のシステム内における行動（例：取引範囲，金額制限，利用コマンドなど）が正当な範囲か否かを確認する。 2.3　利用者のファイルへのアクセスの確認 利用者とファイルとの対応をチェックし，ファイルのアクセスが正当な範囲か否かを確認する。 これらのコントロールはオペレーティングシステム，各種コントロールプログラム，アプリケーションプログラムなどにより実行される。	・周辺装置などにおけるデータ保護機能外部記録装置への書込禁止 ・システム資源の分割 ・資源アクセス管理プログラム ・レコード単位，データ項目単位の機密保護機能
	3. 暗号化 3.1　暗号化の必要性 (1) 通　信：通信の媒体にあるケーブル類は，多様な個所に設置され，全てにわたって通信を盗聴されないよう防御するのは困難である。また，マイクロウェーブ回線や衛星通信回線などの無線通信方式では必要な設備を備えた不法者の傍受を防ぐ手段は困難である。このためには暗号化が有効な手段である。 (2) ファイル：企業秘密など重要なファイルのデータをハッカーなどの不法侵入者から防御するためにはデータ自体の暗号化が必要である。 3.2　暗号化の方法 (1) 方　式：① 慣用暗号方式　：DES（Data Encryption Standard）方式など ② 公開鍵暗号方式：RSA（Rivest Shamir Adleman）方式など (2) 手　段：ホストコンピュータ上のプログラムでも実現できるが専用の暗号装置を利用することによりホストへの負荷をほとんど増やさずに，暗号化システムを構築できる。	・回線暗号装置

（次頁へ続く）

表３－６　（続き）

脅威の内容	望ましい安全対策	セキュリティ機能
	4. 監視・記録 (1) 次のモニタリング機能を設け監視・記録を行う。 ① アクセスモニタリング機能（不正アクセスの監視） ② コンソールログ機能 ③ システム使用状況記録機能 ④ アプリケーションプログラムに組み込むモニタリング機能 (2) 次の管理を行う。 ① 設備：定期巡回による早期発見 ② データ・媒体：保管設備の施錠・使用・保管・破却の許可制度	・端末のジャーナル取得 ・ホストシステムログ取得
	5. 複数のコンピュータシステムを接続したシステムで，かつ専用のコンピュータ室に設置していないコンピュータシステムのためのプログラムおよびデータの不正変更の防止機能 (1) CPU相互接続においても，端末と同様に相手方CPUからのアクセスをコントロールする。 (2) CPU相互接続においても，許諾事項以外については相互独立，相互不可侵とする。	「2. アクセスコントロールの実施」の項に同じ
	6. 要員管理 (1) システム開発にあたり，複数の人によるシステムテスト，重要ファイルへのアクセス制限など，内部牽制，内部統制上充分なチェック監視機能をシステムに盛り込む。また定期的に監視状況のフォローアップを行う。 (2) コンピュータシステム関係者の就業管理・健康管理・精神衛生管理・カウンセリングなどの管理面で配慮し，不正行為が発生しない環境を醸成する。 (3) 機密保護・機密ファイル取得・職務権限などの社内管理規定を明確に定め，これを周知徹底させる。	

出典：「コンピュータ・セキュリティ対策へのアプローチ」（㈶日本電子工業振興協会）より作成

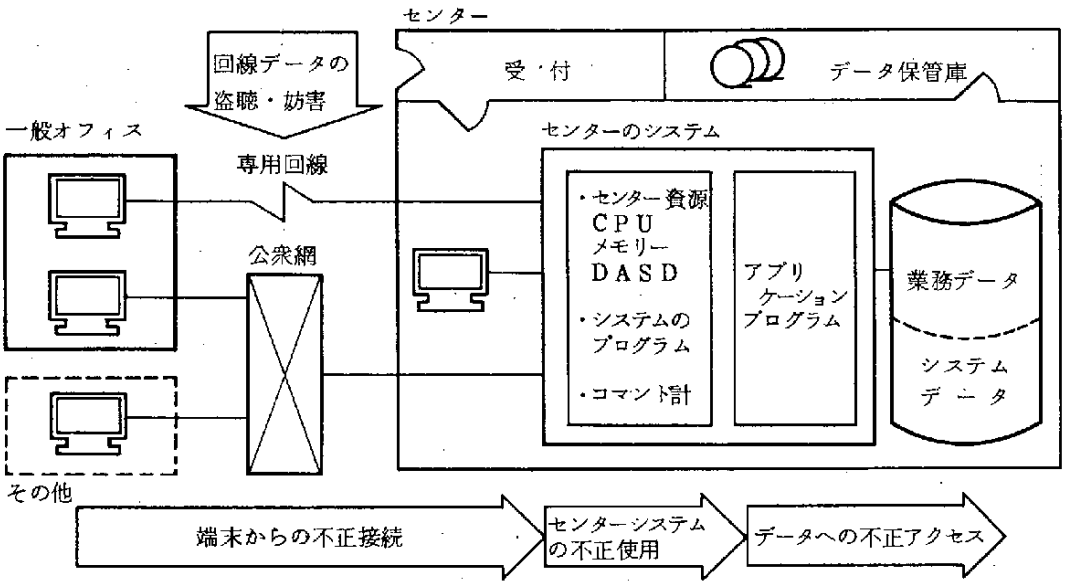
3.2.2　脅威への対応例

最も一般的なオンライン・システムにおける脅威の例は次表の通りであるが（表３－７），この内「データへの不正アクセス」については最も直接的かつ広範な被害をもたらすものであり，様々の対策が実現している。

データはユーザー資産としてのプログラムをも含めるものであり「アプリケーション・プログラム・業務データ」と「システム・データ（ユーザー登録簿・パスワード登録簿）」に大別される。データへの不正アクセスは単なる情報の入手にとどまらず，改ざん・破壊といった脅威を意味するものであり，技術的にはアクセス制限・パスワードの様なシステム標準機能やアクセスを制御する特別なソフトウェアを組み込む事によって対応しているのが一般的である。（表３－８）

この対応策はいわば論理的なアクセス・コントロールともいうべきも

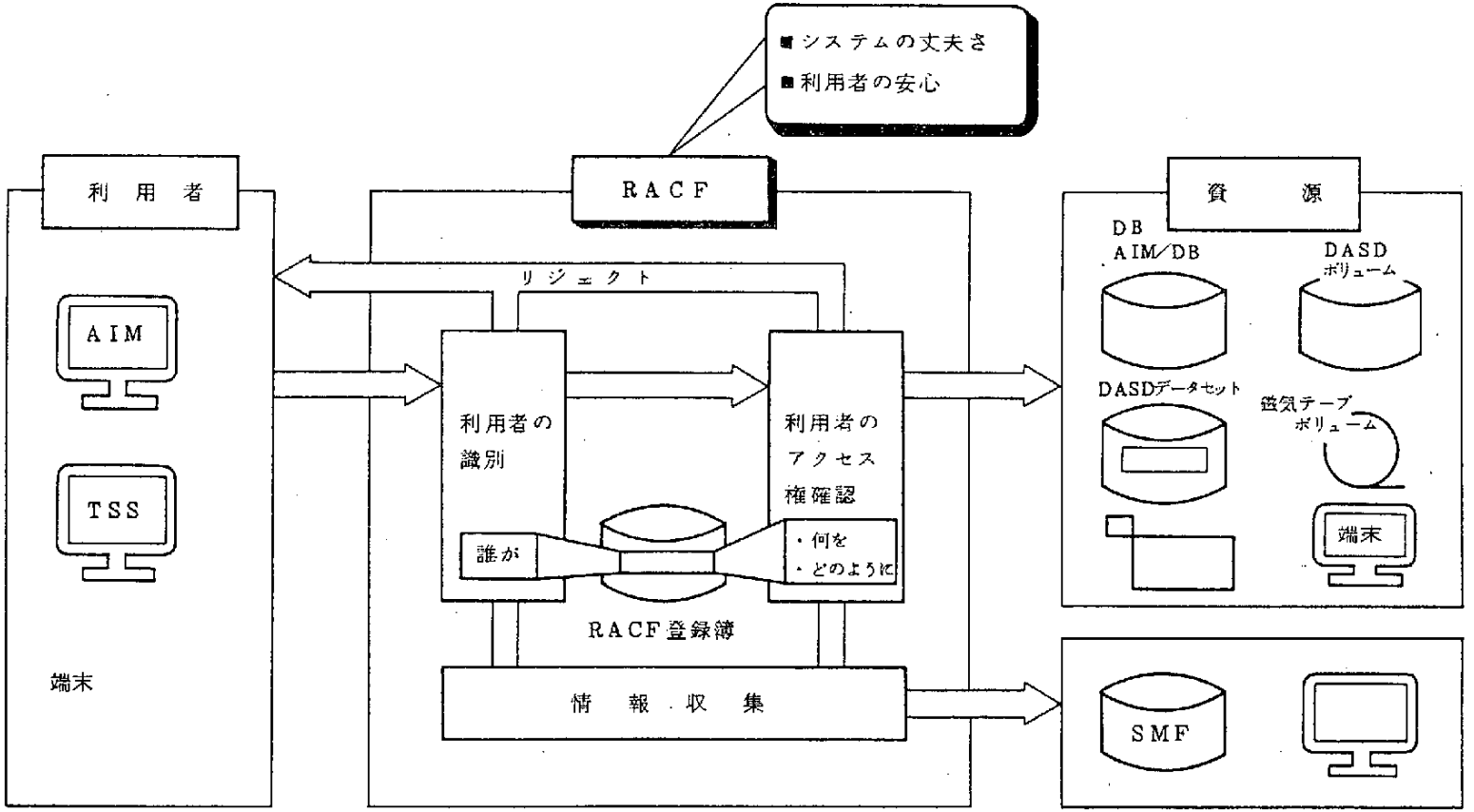
表３－７　脅威の例



注）⇨：脅威

ので，十分効果的である為には，システムへの組み込み方が適切であるかどうか，並びに運用管理の為の規約が十分出来ているか等の環境整備がなされている事が前提である。システムの内的保護機能の充実には，当然コストの増大をもたらす事になるが，コンピュータ・システムの構成要素が広範になればなる程環境整備に対する費用投下も増大し，現状においては必ずしもトータルな対策がとられてはいないといえよう。（表－９）（表３－10）

表３－８　制御ソフトウェアによる対策



RACF：Resource Access Control Facility

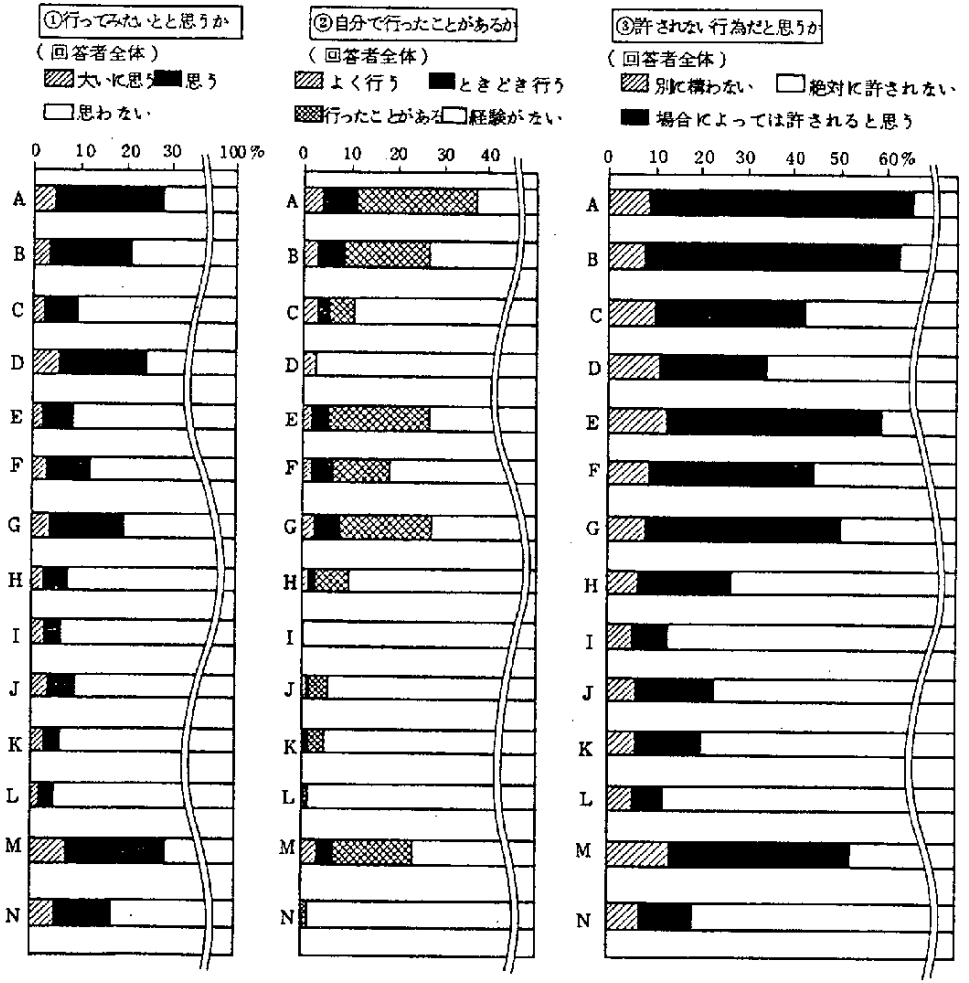
表３－９　安全対策への取組方針の状況

取　組　方　針	企業数	百分比
いかに費用がかかろうとも，安全対策は進める	9	0.8
効果を中心に考えて，多少費用がかかろうとも安全対策を進める	273	23.7
費用対効果を考えて，プラスになるものについては安全策を進める	647	56.2
費用がかかるので，当面は安全対策は取り入れない	151	13.1
安全対策に対する投資は全く考えていない	21	1.8
そ　の　他	21	1.8
無　回　答	29	2.5

出典：「コンピュータ関連の不正行為等に関する意識調査結果概要」
（警察庁　昭和61年12月）

表３－10　コンピュータの不正利用に関する意識

コンピュータ関連の不正行為 または不正行為の周辺的な行為
A 勤務先（学校）のシステムに入っている他人のファイルの内容をのぞきみる。
B 勤務先（学校）のシステムに入っている他人のファイルの内容をアウトプットする。
C 勤務先（学校）のコンピュータ・ルームなどにたまたまあったプログラムリストやフロッピイディスクを持ち帰える。
D キャッシュ・カードやクレジット・カードなどの磁気カードの磁気ストライプ部分の内容を解読する。
E 自分のＩＤや暗証番号を他人に教える。
F 勤務先（学校）のシステムに入っているデータやプログラムを他人に見せたり渡したりする。
G 自分以外のＩＤやパスワードを用いてコンピュータにアクセスする。
H 他人の作ったデータやプログラムなどの内容を勝手に書き換える。
I 給与や人事ファイルなどの個人データを意図的に書き換える。
J オペレーティング・システムやシステム管理ファイルの内容を勝手に書き換える。
K 現に業務（研究）に用いられているシステムに架空データを入力して，架空の伝票や書類を作成する。
L 他人のフロッピイ・ディスクを磁石などで消去する。
M 業務（研究・勉学）とは無関係の目的で，勤務先（学校）のコンピュータを利用する。
N アクセス権限を与えられていないコンピュータシステムにＩＤ番号などを想像して電気通信回線を通じてアクセスする。



出典：「コンピュータ・セキュリティ対策へのアプローチ」
（㈱日本電子工業振興協会）

3.3 法制化への所見

現行刑法の改正によって，コンピュータ犯罪における不正利用に対する処罰規定が新設された事はユーザー，メーカー何れの立場に居る者にとっても朗報である。データの不正入手，不正アクセス等に対しても，近い将来当然何らかの刑事法的対応が講じられる事を期待するがしかし反面，対象がコンピュータという極めて複雑なシステムである為により包括的な具体立法が本当に可能であるのかという疑問をも禁じ得ない。前述の様にコンピュータはシステムとして機能するものであり，コンピュータ犯罪の類型も複雑多岐に亘っている。更にコンピュータが利用される様々の社会システムの範囲も極めて広範になり，恐らくは従来の犯罪類型だけでは解釈し難いものも出てくると思われる。加えて昨今の急速な技術によってコンピュータの構成要素そのものにとどまらず，利用形態にも大きな変化が表われつつある。法的対応のテンポがこの様な時代変化に追随できる保証は殆どなく，むしろ後手に回る事も予想される。こうした状況をふまえ，各種対策立案の為の課題は次の様に要約される。

第一点は，ユーザーの業種環境や固有環境の相異により，必要とされるセキュリティ対策のレベルが異なり，標準化が困難になるということである。たとえば，金融，自治体，流通と各業種とも個人データを蓄積しているが，金融においては，個人の金融財産そのものに近いし，自治体においては，公的に正当性が保証された個人のプライバシーであるし，流通業においては，企業機密のマーケット情報である。この性格の違いが犯罪の質や影響範囲に差を生じさせる。このため，ユーザーがメーカーに求めるセキュリティ対策レベルが，業種によって異なっているのが現状である。また，同一業種であっても，個別ユーザーの環境の違いにより犯罪の発生ポイントやその質が異なり，ユーザーの求めるセキュリティ対策も異なっていると考えるべきである。

第二点は，技術的な限界である。技術的なセキュリティ対策は，現状においても個別機能毎に標準的なものがあり，さらに創意と工夫により，よりレベルの高い対策を取ることが可能であるが，一方では，セキュリティ対策はチェックを厳重にするため，事務処理やコンピュータ内の処理その

ものの効率化を，阻害する要因でもある。このため，技術的対策の一律適用は，本来のコンピュータ導入目的と相反することにもなりかねない。さらにメーカーとしては，ユーザーの求めに応じて，より高度で複雑なものを提供できるが，その仕組を管理しているユーザー側要員の悪意に対しては，有効な対抗策を提供することは困難である。

第三点は，セキュリティ対策には費用がかかり，積極的な意味での利益を生み出さないことである。運用管理面やソフトウェアでのセキュリティ対策には，システム規模や企業規模に関係なく費用がかかる。このため，対策の一律義務化は，小規模企業にとって投資負担比率の増大を招き，競争上の不利益をもたらすことになる。極端な場合，小規模企業は，高度情報化に二の足を踏むことになりかねない。

この様にこの課題は極めて複雑な側面をもっており，現実に効果的な法対応にはかなりの検討が必要であろう。そしてそのアプローチについての所見は次の通りである。

まず，検討は，コンピュータの個々の構成要素別になされるよりもシステム全体としての保護の観点からなされるべきである。特に昨今の様にコンピュータ・システムが様々の付加価値を備えてきている現実においては，個々の犯罪類型では所詮，処しえない課題が次々と想起されてくる事に充分留意しなければいけないと考える。

次に法制化は，対策面ではなく，犯罪や定義面や適正な量刑体系の確立に重点を置くべきではないか。コンピュータ犯罪は，キー操作するだけで実行でき，犯罪の直接行為が軽いため，今後，マニア的なものも増えてくる。そのため，犯罪行為としてのコンピュータ犯罪を明確に定義しておくことが望まれる。また，犯罪行為が軽くても，その影響が重大なものが多いため，影響範囲を考慮した量刑体系の確立が望まれる。特にデータ盗難などは，事件が解決しても，データがコピーされ流布されてしまえば，被害の回復が不可能であるため，適正な量刑が必要である。

対策面においては，法制化には問題があると思われるため，やはり安全対策基準の制定で対応すべきであろう。この安全対策基準は各省庁から個別に出すのではなく，一本化し，むしろ業種別に制定されることを望みた

い。これにより全ユーザーにとってセキュリティ対策の明確な指針になるし，メーカーにとっては，標準的なセキュリティ対策製品の開発のよりどころになる。

以上述べてきた様な諸々の環境の整備を見ながら，メーカーとしてはより標準的なセキュリティ対策製品の開発を進め，トータルなコストの削減を図っていきたい。

そして具体的にユーザーにおいて，セキュリティ対策を講じる時には，安全対策基準とメーカーの標準製品を基礎に，ユーザーの固有環境と方針に合致した適切な対策を，ユーザーと協力して構築していくことになる。また，ここで構築するセキュリティ対策は，第三者による外部犯罪対策として強力であるほど，犯罪の実行者が内部関係者以外に考えにくいという状況を作り出し，これが，ひいては内部犯罪の抑止に繋がっていくと考えられる。

4. セキュリテイ・システムの限界について

㈱オリエント ファイナンス　小泉耕一郎

4.1 はじめに

６２年の現行法の一部改正に際してコンピュータに蓄積された情報の不正入手・漏示，コンピュータの無権限利用などは，情報保護一般，他の類型の無断利用についての論議が尽くされているとはいえないとして，対象からは，外された部分である。

ここでは，コンピュータにおける情報の不正入手に不正漏示及びコンピュータの無権限使用の問題も加えて，コンピュータ・セキュリティ・システムによってコンピュータ犯罪を抑止し得るかを考察するものである。

4.2 セキュリティ・システムのあるべき基準

コンピュータ及び通信の普及は，官庁や企業等の各組織の末端にまで及び，その業務範囲が著しく拡大・複雑化してきた。

もともとセキュリティ・システムに課せられた要件は組織内の規程・基準・権限等と連関し，業務処理の健全性・効率性等を高次元で安定して実現することをねらったものであると考えるが，しかし，これを更に具体的にセキュリティ・システムのあるべき姿が何であるかを一律に定義しようとすることは難しいと考える。

その理由は，今日まで「通産省の電子計算機安全対策基準」が行政指導的な立場を脱し得ないように，セキュリティ・システムに課せられた要件を特定しようとしても，それはコンピュータを利用する組織の置かれた立場・環境・特性やコンピュータ・システムの形態等の諸要素によって，個別に規定されるからである。

従って，コンピュータ・システムの開発や運用等に関する基本的な部分は別として，セキュリティ・システム全般については各組織の自主性によらざるを得ない。この事から，各組織はコンピュータシステムの健全な運営を図るためセキュリティ・システムを独自の立場に立って，能率性・経

済性・安全性の観点から定義しているのが実情であろう。

4.3 能率性・経済性と安全性について

コンピュータ・システムはその機器性能の向上やソフトウェア技術の向上によって業務処理の効率化の有力なツールとしてのみでなく，事故・過失・犯行を軽減する一方，検証する道具としても活用されてきた。その結果として，事故・過失・犯行が減少すれば，それだけ能率の向上と費用・損失の引き下げに役立っている。しかし，コンピュータ・システムの能率性・経済性・安全性は相互に並行する面と矛盾する面とを持っており，特に今日の様に，システムの形態が多様化・複雑化し，しかも社会的に与える影響も大きくなるにつれて，信頼性への要求が運営上で重要な位置を占めてくると，この矛盾する側面の傾向はますます強まってくることになると考える。一般的にハードウェアやソフトウェアによる業務処理の機械化・自動化は本来の目的を飛び越えてコンピュータ犯罪の導体として大いに濫用されて，コンピュータ・システムの安全性を脅かしている。そこで，安全性の強化を図ろうとすれば能率性・経済性に真向からぶつかることになる。コンピュータ犯罪防止のための組織・手続きはこれをまともに実施すれば多大の時間と手数を要し，業務処理の効率を著しく阻害しかねない。例えば，一貫したデータ処理をただ一人に専属させず数人に分担させることを原則とする内部牽制の実施は望ましいが，プログラマはたとえ自分の作ったプログラムについても勝手にふれることは犯行防止上好ましくないとして，実行中のプログラムに障害が発生した際，プログラマがかけつけても監督者の許可を得て，第三者の監視下でなければプログラムの補修をさせないという規定を小規模のコンピュータ処理に押し付けると，システムの円滑な運営を妨げる恐れがある。

また，磁気テープ等のライブラリからの持出しが管理者とライブラリ担当者の承認を条件として行われ，その出し入れの記録が克明になされることは当り前であるとしても，管理者がその記録を四六時中調査して，怪しい点はないか検証を要するとか，保管された磁気テープの実際在庫や入出庫の内容をタイムリに記録と突き合せることを求められると大変な作業になる。

従って，これまで記述した様にセキュリティ・システムの目標は能率性・経済性と安全性の観点でとらえる時，コンピュータを所有する組織はそのバランスの上に設定すると共に規定や権限等によって補足しようとするのが現実と考える。

4.4 セキュリティ・システムでの犯罪抑止が難しいと考えられる事象

前項で述べてきた能率性・経済性と安全性の視点から見たセキュリティ・システムの難しさに対し，視点をかえて技術的側面から実務上で想定される事象をとり上げたい。この事はこれまでに当委員会ですでに問題提起している（６２年９月）が改めて[1]情報の不正入手，[2]情報の不正アクセス，[3]コンピュータの無権限使用について，セキュリティ・システムの対応が難しいと考えられる点である。

(1) 情報の不正入力

① プログラムのロジック上の盲点をついたデータの入力

（コンピュータ自動チェック機能の限界）

コンピュータの自動チェックの体系は(a)項目チェック，(b)レコード内チェック，(c)簡易レコードチェック，(d)マスターチェックに概ね大別されるが，いずれも許容範囲内であればエラー又はアラームの形ではじき出せないケースが多い。この様なデータを不正に入力された時，速かな犯罪発生の探知は難しいケースもあり，事後検証（例えば，棚卸・残高照合等）までの間，抑止できずに進行させてしまう可能性がある。

（参考：チェックシステムの形態）

(a) 項目チェック

対象となる項目単独で，その精度を図るもので，コンピュータ処理対象としての妥当性を確保する事には十分だが，論理的な意味での信頼性の確保は困難である。

ⓐ 桁数チェック　ⓑ 属性チェック　ⓒ 形式チェック

ⓓ 範囲チェック　ⓔ 突合チェック（候補テーブル値との突合）

(b) レコード内チェック

対象とする情報レコード内で相互関連の妥当性をチェックするもの

で，数値項目の精度向上に効果がある。

ⓐ 関連チェック　　ⓑ 計　算

(c) 簡易レコードチェック

主として，チェック単位毎に複数の情報レコード間の関連チェックするもので，数値項目の精度が飛躍的に向上し，データぬけ・データのダブリ等に対する牽制が出来る反面，チェック集計に人的作業がかなり発生する。

ⓐ トータル・チェック

ⓑ シーケンス・チェック

ⓒ ダブリ・チェック

(d) マスター・チェック

予めマスターとして登録されている情報によって，新規情報の精度を向上させるもので機能的には，突合チェックと同様だが，判定対象をファイルに持つために範囲が広い場合でも可能であるが個別のマスター登録にかなりの負荷がかかる。（存在チェック）

② 公衆回線のネットワーク外からの入力

公衆回線によるネットワーク外から端末を操作して何らかの方法により取得した端末番号（許可された）とセンター呼び出しダイアル番号を使って，センターにデータを不正に入力するケース。（図４－１参照）

この場合，不正行為の発見にはロギング・データ又はジャーナルの精査，不正端末の発見についてはダイアルの逆探知等が考えられるが，このケースを抑止することは難しいと考える。

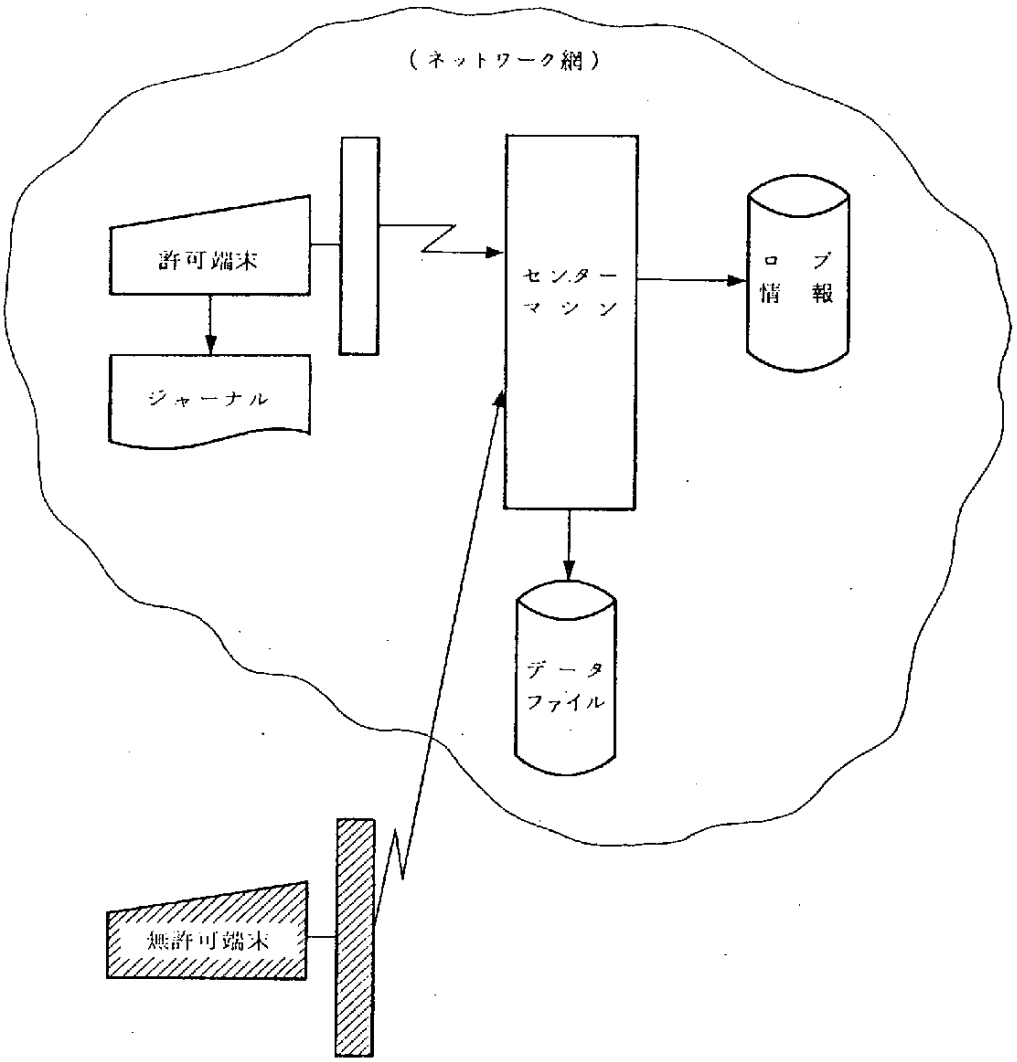


図 4 － 1　　不 正 入 力

③　プログラムの不正入力

プログラム仕様に基づいて作成されたプログラムが所定の手続・規定

等に基づき，数次のテスト段階を経て完成された時，それが結果的にプログラム中の１ステップ又は１つの定義に仕様と異なるロジックを有していたが，通常のデータでは関係なく正常に処理された。

しかし，例外的なデータ又は故意に作られたデータにより，これが障害（不正）の仕掛けになった場合，

“故意” か “過失” か

一般的に１プログラム当り数百ステップから数千ステップに及ぶロジックをもつプログラムが所定のテスト・検査レベルを経て，正しい結果を得たとしても，プログラム・ロジック単位に仕様書との１点・１点の突合せは製造業に於けるボルト・ナットを製品・半製品と同様に１点ごとに検査をする様なものであり，効率性・物理的な面の制約から現実に限界があると考える。

そこに，不正入力の発生の余地を少なからず残しているとしても，発生した事象すべてを故意あるには過失と決めつけることは問題がある。

(2) 情報の不正アクセス

コンピュータの運用上，その使用権限は規定された手続又は特別に許可された特定の者にアクセス権を与えるが，コンピュータ・システムの環境によってはファイル単位の許可やアイテム単位の許可及びその行動まで規則する必要があっても，運用上でこれをまともに実行することは難しいと考える。

例えば，運用上で障害が発生し，その原因追求の為に，データの分析等が必要な時，その取扱い範囲によっては時間的・物理的等の制約から必ずしも特定の者に限定して行わせることが難しく，逆にそれを前提にして基準を定め運用しようとすれば，運用の非効率を招くことになると考える。

(3) コンピュータの無権限使用

コンピュータの使用権限者とは必ずしも単純に特定化することは難しく本来，業務上の権限や取扱い範囲によって許可されるレベルの規定がきめ細かく定義されて，その使用者を限定するものだと思う。例えば

ⓐ 組織上でコンピュータ・セクションに所属する者

ⓑ コンピュータ・セクション又はそれ以外のセクションに所属し，業務

上の権限の範囲で端末操作を許容されている者。

ⓒ 上記の者で特定の端末操作だけ許可されている者。

ⓓ ファイル又はアイテム単位の端末によるアクセスを許可されている者。

ⓔ パスワードを有する者 等

しかし，この基準の定めいかんによっては既存の組織や権限等やシステムの運用効率に与える影響は大きく，慎重な対応が必要である。

4.5 セキュリティ・システムの限界

これまで述べてきた様に，今日コンピュータのハードウェア技術・ソフトウェア技術・通信技術等の進展を背景として，アプリケーション・ソフトや情報処理全般に関し，その範囲が拡大・複雑化していく中にあって，情報処理が常時安全に取り扱われるのに必要な基本的な基準と技術的な発展は必要であると思うが，前記の様なコンピュータ技術の著しい進展と共にますます多様化する情報処理に対し，コンピュータを所有する組織はその都度，かなりの負荷をかけてセキュリティ・システムをメンテナンスする必要がある。

しかし，この事を前提に考えるとしても，情報処理の技術的進展と巧妙化するコンピュータ犯罪の手口を想定する時，常にその防御策を先行させようとすることにはかなり難しく，いつの時代もその間に隙間が存在し得るのが現実であると考える。

現在，コンピュータ犯罪の抑止に対して，刑法化の積極論・消極論のある中で，今回の改正（６２年６月２２日施行）で積み残された①コンピュータにおける情報の不正入手・漏示，②コンピュータの無権限使用等を検討する時，本来もっと実務に即した具体的な根拠や事象をもって討議されるべきである。

つまり，コンピュータを所有する組織の置かれた環境や立場の違い等を一面的且つ共通的にとらえたり，単純なネット・ワークを前提にしたりする事は実態を見失うことになりかねないと考える。

しかも，日進月歩する情報処理化を考えるとむしろ，セキュリティ・システムと刑法は相互に関連して間隙をうめ，コンピュータ犯罪の抑止のた

めの車の両輪として存在させる必要があると思う。

従って，当委員会はコンピュータのもつ脆弱性や運用の実態及びセキュリティ・システムの限界等について論議をつくさずして，刑法化積極論・消極論について討議する。即ち，法律的側面に重点を置いた検討を優先させることは，本来の主旨にかなった結論を導き出すことを，著しく困難にさせると考える。

4.6 今後の刑法化にむけて

今回の刑法の一部改正に於いても，伝統的な法の適用の難しい点を補足して規定したことや情報保護一般，他の類型の無断利用が今日まだ十分討議をつくされていない点，更にコンピュータによる情報処理化が複雑化・多様化している中で，巧妙化すると想定されるコンピュータ犯罪に対処するには，可能な限りコンピュータ運営の実態をふまえて討議・検討されなければならないと考える。

5. 通信システムにおける不正行為の脅威とその対策

日本電信電話㈱　土屋守之助

5.1　はじめに

コンピュータ及びこれと結合した通信システムにおける情報の不正入手，不正漏示，システムの無権限使用等不正行為が発生する潜在的脅威と，これを防止するための対策につき，まず問題となり，かつ，影響も大きいと考えられるのは電気通信事業者 — 具体的には，現在は主として 日本電電 — の提供する公衆型の通信システムである。サービスの形態としては，電話，専用，データ通信，デジタル・データ伝送等を内容としている。これらの通信システムは，隔地者間における情報の送受を行うものであり，その通路は，日本国中東西南北縦横に存在し，当然ながら情報の送り手又は受け手の管理支配下に常にあるとは限らない。そのため電気通信システムを利用した情報はその送受の過程で，情報の不正入手（見読，盗聴），不正使用，不正漏示等の不正行為の脅威に常にさらされているのが実状である。又いったん送受された情報がコンピュータ，ＦＤ（フロッピ・ディスク），ＭＴ（磁気テープ）等に蓄積，保管されている段階においても，内部者からのものも含めて不正行為の脅威が存在する。

以下では，まず以上のような不正行為に対する潜在的脅威の実態と防護策について明らかにしたい。次にこれらの不正行為に対する法的評価を行う。最後に以上に関連する若干の問題につき言及したい。

5.2　不正行為への脅威

(1)　有線電気通信系

電話，データ通信等における情報伝送路の大宗は有線系のシステムである。尤もこの有線系システムの中間に無線系のシステムとしてマイクロウェーブ路が設置されることもある。全国主要都市に所在する電話局相互間を結ぶ伝送路は主として同軸ケーブルや光ケーブルが用いられている。電話局から各事業所や家庭へは，各ユーザーの需要に応じて，必要な容量の回線が伸びている。その形態は現在，通常交換局から一対の銅線である。

伝送路は同軸ケーブル又は光ケーブルであり，これに対する不正行為（見読，盗聴，漏示，不正利用等）は技術的又は経済的にはなはだ困難であり，実例はないようである。あるのはケーブル切断という形態である。同軸ケーブルや光ケーブルでは物理的には一対の回線に何百，何千の通話やデータが搬送という形で相乗りしており，切断以外不正行為の入り込む余地が少ない。又これらの通信路は，ほとんど地下管路に収容されており，この点も不正行為が行われる可能性を小さくしている。これに反して，電話局及至交換局から，各ユーザーに伸びている市内線は，通常各ユーザーごと一対の専用の通話路を形成しており，そこも流れる通信内容は個別に識別可能である。又市内線では交換局からユーザーの事務所又は居宅の直近の電柱まで地下又は空中を通過するが，直近の電柱からは空中より引込むケースが多い。ただし都市等では地下から引込まれることもある。まずこの空中線がねらわれやすい。不正行為の方法としては，対象回線にマルチに有線を接続するか，小型発信機を仕組む等の方法がある。最近世間を騒がせた町田の緒形宅事件（注1）も，国立の上田宅の件（注2）も，ここで問題が発生している。

以上のほか，不正行為の可能性がするのは，マンションやビルの配線盤と各事業所や家庭の保安器部分である。配線盤は電柱等から引き込んだ複数の回線を各戸に分配するための切り分け装置であり，保安器は避雷のため各ユーザーの回線に接続されており，その軒先などに取付けられている。不正行為の方法としては配線盤の端子付近に，小型無線発信器を取り付けるか，端子に有線回線を接続延長する等の方法がある。又保安器に対しては，盗聴発信機能のある，外観上普通のものと変わりのないものに取替える等の方法がある。

以上の不正行為に対する脅威は，電話回線によって伝送されている限り，データ通信の場合も全く変わりはない。

以上は，データの伝送部分についてみたのであるが，目を転じて屋内ではどうか。まず電話不換局はどうか。ＮＴＴはじめ電気通信事業者の管理する施設は入退室をはじめ厳しく管理されていると思われるので外部からの脅威はかなり小さいと思われる。かえって，内部者による脅威のほうが

問題となろう。我国初の本格的コンピュータ犯罪と言われた札幌ＣＤ事件（注３）がその実例である。次にユーザーの屋内についてはどうか。近畿相互銀行事件（注４）や福岡銀行通帳偽造事件（注５）などずい分と実例がある。

(2) 無　線　系

マイクロウェーブによる固定無線に対する不正行為の脅威は前項で述べた局間中継線のケースと同じである。ここでは，移動体通信を扱う。移動体通信に対する脅威としては，自動車電話盗聴，警察無線盗聴，衛星通信無断傍受等がある。移動無線の代表は自動車電話があるが，最近自動車電話の盗聴器が市販されており，盗聴に関する苦情も発生している。今後自動車電話の普及拡大及びデータ伝送を含む機能拡大が想定される中で，不正行為に対する脅威は除去しがたい状況にある。自動車電話においては，盗聴等不正行為が行われた場合，仲々顕在化しずらく，取締りが困難であるという特徴がある。コンピュータと結合したシステムのセキュリティという点では将来の課題となろう。

5.3　不正行為の防止策とその限界

以上の不正行為はどのように防ぐか，有効な手段はあるのか。この点で図表５－１に示してみよう。セキュリティ対策中，マンホールの蓋の棚づけ，架空端子ブロック函の施錠；端子函の施錠等は対策として効果は想定されるものの，作業実施面や管理権限等の問題があり実施できたがたい状況にある。通信事業者の局内，ユーザーの屋内では種々考えられ実行されているものの，一種の例外管理なので，その徹底は困難というのが現状であろう。

図表５－１　不正行為のターゲットとセキュリティ対策

脅威のターゲット	セキュリティ対策
●幹線通信路・局間伝送路	マンホール蓋の棚づけ，架空端子ブロック函の施錠，パトロール
●引込線以下	端子函の施錠・封印；保安器の場所工夫，パトロール
●通信事業者局内 ●ユーザー屋内	施錠，入出管理，管理規程 社員教育，　等　(注)
●自動車電話	デジタル化，暗号化

(注)　富士通ジャーナルNo.１４０号コンピュータセキュリティ特集参照

5.4　不正行為の態様と法的評価

コンピュータと結合した通信システムにおける情報に対する不正行為として，不正見読，盗聴，漏示，不正利用等が考えられる。これらの不正行為により，情報の保護主体に損害を発生させれば，不法行為として民事上の責任原因となると考えられるが，この点は別として，刑罰関係法規の適用関係はどうなるか。この点をみたのが図表５－２である。不正行為としての，不正見読，盗聴，漏示は異論なく，電気通信事業法第１０４条に言う「通信の秘密を侵した」場合に該当する。不正使用は，通常その前提として，不正見読，盗聴を伴うと思われるが，伴わない場合は金銭の領得等他に可罰的行為がない限りそれ自体可罰的ではないと考えられる。今回の刑法改正（６２年６月）では，これらの不正行為に対する可罰規定は新設されなかったが，多くのケースでは，電気通信事業法等既存法令によってカバーできると思われる。

図表５－２　不正行為に対する刑罰規定

不正行為の態様			刑罰規定
電気通信事業中に有線か無線かを問わず通信を取り扱う者に有る		不正見読，盗聴	従事者：２年以下の懲役又は５０万円以下の罰金 非従事者：１年以下の懲役又は３０万円以下の〃 （電気通信事業法第１０４条）
		漏示	
		不正使用	適法に入手した情報を不正に使用しても，他に可罰的行為を伴わない限り，罰則の適用はないと考える。
その他の通信	有線	不正見読，盗聴，漏示	従事者：２年以下又は３０万円以下 非従事者：１年以下又は２０万円以下 （有線電気通信法第１４，１５条）
		不正使用	上欄不正使用の欄に同じ
	無線	不正見読，盗聴	不正見読のケースは存在しないと思われる。 盗聴については，電波の特性上通常のケースでは不可罰と考えられる。ただし，積極的意欲の伴うケースについては可罰・不可罰の両説がある。（平井正俊「電波法要説」242頁参照）
		漏示	従事者：２年以下又は３０万円以下 非従事者：１年以下又は２０万円以下 （電波法第109条）
		不正使用	電波法では「窃用」すれば可罰的である。

5.5 いくつかの問題

(1) 通信の秘密保障はデータ通信に及ぶか。

前項で，通信システムに対する不正行為（見読，盗聴，漏示。不正使用等）の態様と法的評価をみたところであるが，その中で明らかなように，これらの不正行為は，主として電気通信事業法，有線電気通信法及び電波法における通信の秘密保障の諸規定（電気通信事業法第104条ほか）によって，処罰の対象とされていると解せられる。ところがこれらの保障規定はデータ通信には及ばないのではないか，あるいは及ぶとしてどのような解釈でそうなるのかという疑問が出されることがある。そこでこの点を明らかにしたい。

まず電気通信法第2条に「電気通信」に関する定義があり，それによると，電気通信とは，「有線，無線，その他の電磁的方式により，符号，音響又は影像を送り，伝え，又は受けることをいう」とされている。データ通信については，その伝送過程は明らかに，本条にいう，「……符号……を送り，伝え，又は受ける」場合に該当する。伝送過程にない場合つまり，データの蓄積，変換，加工などの処理の行われる場合はどうか。この場合に上記の定義から外れてくるという根拠はない。データの蓄積，変換，加工などの処理は電子計算機等により電気通信評線に接続なれた形で行われる以上，電気通信が行われる過程で一体的に行われるものであるから，「電気通信」の中に含まれるものと解せられる（郵政省電気通信監理官室「電気通信関係法規詳解」下巻315頁）。この電気通信事業者がサービスとして提供している場合は，電気通信事業法第104条にいう「電気通信事業者の取扱い中に係る通信」に該当する。従って平たく言えば，ＮＴＴなど電気通信事業者の回線とオンラインに結ばれているコンピュータの通信システムでは，その通信のすべて — 初めから終りまで蓄積データも含めて — が本条の適用対象となると解せられる。

(2) 通信終了後の通信の記録ないし書類等は秘密侵害の対象となるか。

通信の秘密の保障規定である電気通信事業法第104条によると保障の対象は「電気通信事業者の取り扱い中に係る通信」とされている。そこでこの「取り扱い中に係る」の意味が問題となる。具体的には，配達の終わっ

た電報原書（現在はＮＴＴのコンピュータ内に一定期間保存されている）や通話終了後における電話交換値（現在電話は自動化しているので，100番通話やコレクト・コールなど特殊な通話に限り交換証を作成している。）さらには，通話の明細記録などをどう解するかである。コンピュータに結合したデータ通信に関して言えば，オンライン・データ伝送終了後のさん孔テープ，ＭＴなどが問題となろう。

この問題については，通信終了後の通信内記録ないし書類等はすでに取り扱いが終了しており，保障の対象外であるとする考え方も出てくるかもしれない。しかし，そう解すべきではなく，保障の対象とみるべきであろう。その理由として，第１に，もし対象外とするならば，秘密というものの本来的性格上，秘密保障の趣旨が全く否定されかねないからである。通信終了後その通信記録や書類が野放しでは秘密保障の意味がないとさえ言えるのではあるまいか。第２に，こうした記録ないし書類等の内容も，電気通信事業者に保管されている間は，「取り扱い中に係る通信」の内容として電気通信事業法第104条の秘密保障の対象と解すべきであろう。

〔注釈特別刑法(6)交通通信法編Ⅱ — 347頁（河上和雄氏）〕

（注１）　昭和６１年１１月２７日　日本共産党 緒方靖夫 国際部長の自宅から約 ２００m 離れた端子函内で緒方氏の収容回線に別の電話線がマルチに接続され，それがあるマンションに引き込まれていることが判明した事件（昭和６１年１１月２９日付朝日新聞等）。

（注２）　昭和６２年２月２１日　東京地検は，日本共産党 上田耕一郎 宅直近の電柱から四対ブロック端子（切り替え装置の一種）とコネクタを押収した。同端子内に無線発信器が仕組まれたのではないかとの疑いがもたれた。

（注３）　昭和５５年１２月当時電電公社の職員であった者が，①公社の取扱い中にかかるデータ通信回線から，その交信中のデータ通信音をカセットテープに録音したうえ，これを解読しようと企て局内において北海道銀行のＣＤオンライン通信回線より，伝送中の顧客の氏名，口座番号，銀行コード等を内容とする電気通信である交流信号音を録音した。その後この録音テープからデータを再生・表示させて解読し，公社の取扱い中にかかる通信の秘密を侵害した。②当人はさらにその解読した情報をもとにＣＤカードを作成しこのカードを利用して，北海道銀行支店ほか２か所のＣＤ機から計 １１２万円を引き出した。この事件に対して札幌地方は，当人を①通信の秘密侵害（公衆電気通信法第 112 条：現在の←→電気通信事業法第 104 条に該当する）の罪，②窃盗罪の成立を認めて，懲役２年６月執行猶予４年に処した（確定）。

（注４）　近畿相互銀行の職員で同行のオンラインセンターのデータ処理部門でオペレータとしてＣＤカード発行等の作業に従事していた者がＣＤカードを偽造し，同行梅田支店ほか１３か所で現金自支払機を作動させ現金約 ９００万を窃取した（刑裁月報 vol.14 №10－1982）

（注５）　昭和６１年３月　技師派遣会社から福岡銀行コンピュータセンターに派遣された技術者がデータ処理により他人の口座から自己の正規の通帳へ合計約 1,０００万円を入力し，引出した。

6. テレコミュニケーション・システムと結合したコンピュータに蓄積された情報・資料の保護

中央大学教授　渥美東洋

6.1 はじめに

憲法２１条２項は検閲の禁止と通信の秘密の保護を明文で定める。

これを受けて，通信関係法規である郵便法（８条，９条，８０条），有線電気通信法（９条，１４条），電気通信事業法（３条，４条，104条），それに電波法（５９条，１０９条）が通信の秘密を保護し，検閲を禁止する規定をもっている。

ところで，このうち電気通信事業の前身である公衆電気通信法でも同様の規定がみられたが，当時，公衆電気通信を取り扱っていた電電公社が，法改正によってデータ通信事業も行うことできることになった。

さらに，電気通信事業の民間化と自由化（独占の解消）により，電電会社となり，有力だが，多くの第一種事業者として新たに参入した通信事業者と並んで，電気通信事業者の１つであるにすぎないことになり，この事業分野でも競争の時代に入った。

さて，新たにデータ通信事業の分野が開発されることによって，電気通信事業者は従来の通信システムにコンピュータ・システムを結合し，そこに自己が開発した各種のデータを貯蔵するだけでなく，利用者が通信システムを利用して事業者の用意するコンピュータ・システムに「通信」したうえで貯蔵してもらうことが可能となった。

このとき，発信者と受信者との間の２点間で流れている通信には，従来の音声通信だけでなく，電磁的方式により，符号，映像を用いて行われる通信も含まれ（電気通信事業法２条１号），２点間のこの意味での通信が流れている状況での通信の秘密が同法によっても保護されることには問題はない。

だが，電気通信事業者が用意するコンピュータ・システムに貯蔵されることになった情報が，事業者の「取扱中に係る」通信として同法の通信の秘密の保護を受けることになるのか否かについては明文を欠き解釈に委ね

られている。

テレコミュニケーション・システムに結合されたコンピュータに貯蔵されている情報への不正なアクセスによって，その情報を秘密に入手し，情報内容を他人が知りうる状態に置き，それを放置することは，その情報を保有する者やその情報が自己に関係する者のプライヴァシィーを侵害することになる。

このような形式で貯蔵されている情報のもつ財産的価値の保護は今回の刑法の１部改正によって相当程度はかられることになったが，情報のプライヴァシィーは，情報への不正アクセスを規律しない限り，保護されない。

ところで，「通信の秘密」として憲法や法の保護を受けない情報であっても，憲法３５条は「憲法上保護された領域」にある人のプライヴァシィー保護の射程に入る限り，政府の不合理な捜索，押収から守られることになる。

ここで考えるべきことは，プライヴァシィーへの干渉は，政府にこそ，犯罪の解明，摘発等の場合に必要であることが多いのに，政府はその干渉を憲法で規律されるのに対し，人のプライヴァシーの干渉に合理的で，妥当な利益を政府ほど持っていない私人の他人のプライヴァシィーを侵害する活動が放置されてよいはずはない，という点である。

したがって，テレコミュニケーション・システムに結合されたコンピュータに貯蔵されている情報への不正アクセスは，流れている情報への干渉，不正アクセスであるワイヤタッピングや傍受に当たるとして規律されなければならない。

このように，そのようなコンピュータに貯蔵されることになった情報は，単に財産的利益としてだけでなく，他人に干渉されないで自由に生き，自己の情報を自己コントロールすることができるプライヴァシィー権として保護するべき必要は高い。

しかも，通信法規が憲法を受けて定めた通信の秘密は，通信のもつ財産的利益に着目するのではなく，むしろ個人の自由領域に着目して定義するべき概念である。

したがって，このようにしてコンピュータに貯蔵される結果となった情報を保護する立法の必要は高いことはいうまでもない。

また，このような情報への不正アクセスを規律することによって，コンピュータと結合させた通信システムの完全性はシステムとして保護されることになる。それは，丁度，家屋や事務所という空間内での自由領域の安全性を保護することと同様である。家屋や事務所の中では，人が経済活動を行おうと，精神や思考活動を展開しようと，その活動の性質を問わずに，その空間は「憲法上保護された領域」として，人のプライヴァシィーを守るのに役立つのである。

その結果，精神活動も経済活動も含めた人の全生活が不当な干渉を受けないことになる。このように，通信の秘密とかプライヴァシィーの保護は，精神活動と経済活動も含めた，あらゆる人間の活動に共通の「完全性」の保護を与えるものである。そのため，財産上の利益への侵害，例えば業務妨害や財産的利益の不正入手の前段階の行為が，通信秘密の侵害行為やプライヴァシィー侵害行為として捕捉されうることになり，その結果，コンピュータに貯蔵されている情報内容への信頼を高めることにも通ずるのである。

したがって，通信システムに結合されたコンピュータに貯蔵されている情報を外部の侵害から守る必要は高いことは判明したが，その情報が電気通信事業法4条と104条によって保護されるか否かは別問題である。

データ通信事業を電気通信事業者に認める法改正が行われた以上，データ通信事業の完全性の保護を改正法が考えていたのは当然だとして，そのようにコンピュータに貯蔵されている情報も「通信」として保護されるとする見解もあり，電電会社のとるところのようである。

この解釈の是非をめぐって検討し，このような解釈が成り立たないのであれば，立法による解釈案を真剣に検討すべきことになると思われる。

6.2 通信秘密の保護とプライヴァシィー保護のずれ

先にあげた通信関係法規による通信または信書の秘密の保護は，いかに極端に解釈しようとも，信書や通信のもとになる情報や通信のシステムに乗る以前の状態にあったり，通信システムを通った後の状態になると，その情報にまで及ばない。

ポストに投函する前の封書や葉書は，人の住居や事務所にあっても，通信の秘密の保護は受けない。また，配達後に私人の事務所や住居に置かれた封書も通信の秘密の保護を受けない。だが，その封書は憲法３５条の保護を受けることは問題ない。

通信の傍受，ワイヤタッピングは通信関係法規によって刑罰でもって規律されているが，住宅や事務所内の人の会話の形式をとるコミュニケーションの電子工学的機器をもちいて行う行為はわが国では刑罰によって規律されていない。

このように，通信の秘密の保護とプライヴァシィーの保護とは必ずしも一致しない。

したがって，発信者と受信者の間の通信の過程にある情報と通信の結果としての情報は，性質を異にするのであって，性質の異なるものを同一に保護することには無理がある。

また，通信システムと結合したコンピュータへは，通信システムの端末を利用して不正にアクセスしうることになっているので，コンピュータ・システムに貯蔵された情報を単なる通信の秘密として保護するにとどまらず，テレコミュニケーションの結果としての情報をプライヴァシィー保護の広い射程の中に含めようとするのであれば，何も通信事業者の用意したコンピュータだけに限ることなく，通信システムに結合された他の事業者，さらには個人のコンピュータに貯蔵された情報をも保護すべきことになるであろう。

6.3 『事業者の取扱中に係る通信』の意味

事業者は通信サービスを提供するに当たって通信目的を遂げうるように発信者と受信者との間の通信を可能にしなければならない。発信者と受信者間に直結せず，間隙が生じ，その間に事業者が介在する場合も「通信」の秘密は持続しているとしなければならない。交換手が交換する場合も，もちろん，通信と郵便が混在する電子メールの場合も，また，電報・電信の場合も，着信・受信者に到達するまでは，「通信」は流れており，継続している。そして受信者に到達した時点と地点で「通信」は終了する。ま

た，発・受信者の通信中であっても，受信者の端末に通信が到達したあと，その端末以遠に設置された私人の関係施設を用いた傍受は，事業者の取扱に係る状態を脱しているので，通信関係法規の保護は受けないとみるのが一般である。

さて電報を例にとると，頼信紙や電報文を示した記録は，通信途上にあるから，着信するまでは「通信」や「郵便」の秘密で保護されることになる。だが，着信したのちそれらの記録が保管されているとき，それは郵政省の取扱中や電気通信事業者の取扱中にかかる信書や通信ではなくなる。

たしかに従業員は，これらの記録に示された情報を外部に漏らしたりすれば刑罰により規律は受ける（郵便法９条２項，事業法１０４条２項）が，それらの文書に示された記録が着信者の手に渡ってしまえば，その記録は私人の通常の「書類」または，「所持品」として扱われることになる。

そこで，電気通信事業者が如何にその管理・保管に当たっているとはいえ，事業者の用意し提供するコンピュータを受信点として着信したあと，それに貯蔵されている情報，およびそこから発信する以前にそこに貯蔵されている情報は，事業者が管理し，保管している「情報」ではあっても，事業者が「取扱中」の「通信」ではないとみるべきだろう。

したがって，それらの干渉は，通信システムに加入者が自ら結合しているコンピュータに貯蔵されている情報への干渉と相違がないはずである。さらにいえば，第三者に自己の情報を託している場合の方が，自己の直接支配に置いている場合よりも本人のプライヴァシィーの保護への期待は弱いとみるべきなのが通常である。それなのに，着信後，第三者たる事業者の保管する自己の情報の方が，自ら通信システムに結合させた自己のコンピュータに貯蔵した情報よりも，法的に厚く保護されるという結論を引き出すのは，相当に困難である。

さらに，チェイン形式でチェインの加盟者からチェイン本部が事業者と契約してあるコンピュータに通信システムを介して送られ，そのコンピュータに貯蔵された情報を，チェイン本部は電気通信事業法４条と１０４条に違反せずに入手・アクセスし，利用し，他に伝達（つまり漏示）することができるとされる法理は何であるのかを検討してみなくてはならない。

もし，チェイン店（本部とは独立の加盟者とする）からそのコンピュータに送られた通信を，本物が途中でワイヤタップすることは，事業者の取扱に係るものであるから許されないことは言うまでもない。コンピュータに着信後そこに貯蔵されている情報も，通信の結果として，過去の通信内容をそれを通して知りうることにしてはならないという意味で，事業者の取扱中に係る「通信」だと仮定しよう。そうすると，事業者がそのコンピュータの保管者以外の者に開示するサービスは，通信の秘密を害することになる。

また，ある者が通信事業者の提供するコンピュータに情報を貯蔵し，その情報に多くの者がある者と契約を結んで接することも，事業者の取扱中にかかる通信であれば，事業者はそれを他に開示することは秘密侵害になるので，かかるサービスを提供することも許されなくなるのではなかろうか。

これらのことが許されるのは，事業者の提供するコンピュータに貯蔵されている情報は，通信以前のまたは通信後の状態にある情報を入力した者の支配下にあり，その者のプライヴァシィーの保護の対象になると考えればよいのではなかろうか。

6.4 通信事業者以外の者が通信システムに結合したコンピュータ・システムの保護の必要性

まず，ある保管情報を発信する前にコンピュータ・システムやその他の文書記録等の形で保管し，あるいは通信の受信後，その情報をコンピュータ・システムやその他の記録保存形式で保存しているとき，この保存された情報を保護すべき必要は高い。

物理的侵入と押収した対象，情報を獲得した対象が有体物でなければならないという２つの要件の充足を求めれば，いわゆるプライヴァシィーは現代の電子または光電子工学の発達した社会では守られなくなることが多くなる。

文書の形式で保管されていた情報をコンピュータの形式で保管し，そのコンピュータ・システムを通信事業者の提供する通信システムに結合させ

ると，通信システムを通したその情報への不当アクセスは法の規律の対象外になるとみてよいのであろうか。

まさに，ワイヤタップは，単に人の口頭の会話だけでなく，コミュニケーションの記録，人が保管している情報全体を侵害するという，大きな脅威となった。このとき，通信システムに自己のコミュニケーション・システムを結合させた者は，その限度で，かつて文書に自己の情報を保管していた状況より，自己のプライヴァシィーを大幅に侵害されてもよいといえるのだろうか。

このとき，通信システムの利用者が自ら用意したコミュニケーション・システムに通常の充分な安全対策を自ら講じているのにもかかわらず，同程度の安全対策しか講じていない通信事業者の提供するコンピュータ・システムよりも，（通信システムを不正利用したコンピュータに保管されている情報への干渉であるのに）何故低くしか，保護されなくてよいのだろうか。

プライヴァシィーの保護という見地から考えるならば，その情報に直接の利害を持つ者が自ら管理している情報を第三者にその管理・保管を委ねた情報より厚く保護すべきことになる。

さて，ところで，次に第一種通信事業者でない者が，通信システムにコンピュータ・システムを結合し，そのコンピュータ・システムを結合し，そのコンピュータ・システムだけを管理・保管して，一般第三者にそのコンピュータ・システムの利用サービスを提供するという場合を考えてみよう。

このとき，まさに，そのコンピュータに自己の情報を預け，そこに自己の情報を貯蔵した利用者のプライヴァシィーの保護はそのコンピュータ・システム提供業者の信頼にかかっている。

このとき，そのコンピュータ・システムに貯蔵されている利用者の情報への干渉は，1つは，テレコミュニケーション・システムの不正利用による場合がある。第2は，コンピュータ・システムの不正利用による場合がある。

テレコミュニケーション・システムの安全性を論ずることができる限度

では，「通信の秘密」の保護という概念が有効に機能する。そこで，通信事業者の取扱中にかかる「通信」の秘密を侵害する限度では，そのコンピュータ・システムへの不正な干渉は電気通信事業法の規律を受けてよい。

だが，第一種通信事業者でないコンピュータ・システムのサービス提供者とその従業員はコンピュータに貯蔵された情報について，秘密を守り，漏洩，開示の禁止を法律上規律されていない。また，そのコンピュータ・システムの安全策が不十分なために，貯蔵された情報への不正干渉があったときにも，電気通信事業法は，それには及ばない。

第一種電気通信事業者が提供するコンピュータ・システムのサービスも基本的には，通信事業に従事せずに，コンピュータ・システムのサービス提供を行う業者のサービスを同質のものであると解さなくてはならない。

第一種通信事業者が提供するサービスであるという理由だけで，コンピュータ・システムのサービスが電気通信のサービスに変容するとみるのは十分な理由を欠いている。

ただ，電気通信サービスを提供する業者が提供するコンピュータ・サービスについては，通信サービスの範囲を超えて，電気通信事業者と同内容の法的保護と規律を加えるといった政策をとって，それを立法化することは可能である。

つまり，例えば，コンピュータ・システムのサービスだけを電気通信事業者の提供するテレコミュニケーションに結合させて提供する業者と従業員には，現行の電気通信事業法104条2項のような義務を課したり，刑法にその義務を遵守させるようにするまでしなくても良いとの政策をとることも，もちろん可能である。そのコンピュータ・システムの利用者の情報への信頼や，自ら保管する場合よりも，弱まることもありうると考えてもよいからである。

6.5 結びに代えて

電気通信業じ法4条と104条が前提とする「通信の秘密」の保護は，通信システムの完全性に由来する概念であって，コンピュータ・システムの完全性に由来する概念ではない。

通信システムへの干渉から生ずる情報への侵害と，コンピュータ・システムへの干渉から生ずる情報の侵害とは，本来別のものである。

通信システムとコンピュータ・システムが結合されたときには，この2つの関係が混同されやすい。

電気通信事業者が提供する通信システムの完全性を保つ必要は高く，したがって，通信システムに自己のコンピュータ・システムを結合させた通信システムの利用者に対しては，通信システムの不正使用，通信の秘密を侵す活動から，そのコンピュータ・システムへの干渉が生じたときは，その干渉は電気通信サービスへの干渉と同様の規律を加えるべきであろう。

つぎに，コンピュータ・システムのサービスを提供する業者のコンピュータの利用者がそのコンピュータ・サービスの完全性を害する方法で，そのコンピュータに貯蔵した情報が害されたときは，コンピュータ・システムの完全性を保護する立法を欠く限り，いかに，そのコンピュータ・システムが電気通信サービスに結合されていても，その干渉活動は規律されない。

そこで，最後に，たまたま，電気通信事業者が自ら提供するコンピュータ・システムを自己の通信システムに結合させているからといって，ここでのコンピュータに貯蔵されている情報について通信システムの完全性を守る法規の保護や規律が及ぶことにはならない。

第一種電気通信事業者の提供する，通信システムに結合させたコンピュータ・システムのサービスには，現在の電気通信事業法に定めると同様の保護と規律をもって，そのサービスの完全性を保つことを意図するのであれば，その意図が明確になされるような立法の明確化が望まれる。

テレコミュニケーション・システムに結合されたコンピュータ・システムの完全性をどのように保護するかについて，今後の周到な立法上の検討が望まれる。

その際，①通信システムに自らのコンピュータ・システムを結合している場合，②第三者の提供するコンピュータ・システムが通信システムに結合されているときのそのコンピュータに預託した情報の保護を要する場合，とは基本的に分離して考えるべきである。

この意味で，現行の電気通信事業法4条と104条の保護と規律が，電気通信事業者が自らその通信システムに結合させてコンピュータ・システム・サービスを行っているときには，そのサービスにまで及ぶとする解釈には相当に無理があるというべきである。

第２部　情報犯罪の脅威とセキュリティ対策等に関する調査

第２部　情報犯罪の脅威とセキュリティ対策等に関する調査

（財）日本情報処理開発協会

1.　調査の概要

1.1　調査の目的及び対象

(1)　目　　的

昭和６２年に行われた刑法の一部改正は，コンピュータ犯罪への早急な対応策として，従来の犯罪類型のすき間を埋めるという方向で行われたため，従来刑法に類似の犯罪類型のなかった「データ，プログラムの不正入手」等をどのように扱うかは，今後の検討課題として残されている。

このアンケート調査は，コンピュータで処理される「情報の不正入手」に関する法制的対応を検討するため，その基礎資料を得ることを目的として行ったものである。

(2)　対　　象

オンライン・ユーザー企業（６1／3に当協会で実施したコンピュータ・セキュリティ実施状況調査の回答企業1,383の中から抽出。）

調査票の発送先数：５９１，回収数：２９７，回収率：５０.３％

調査時点：昭和６３．１．２５

回答企業の概要（業種，規模等）：1.3前文，問１（６９ページ）参照

1.2　調査結果

1.2.1　情報の不正入手に関する潜在的脅威（アンケート 問２）

どのような手口による不正入手の脅威が大きいかというのが，質問の趣旨である。

潜在的脅威の程度を「大・中・小」に区分しているが，このうち「大」と「中」の答えの合計が回答者全体に占める割合を比較してみると，（1.3問２，７１ページ），多いのは，処理作業段階におけるアウトプット情報の複与等（５６％），媒体の持出しによる情報の複与（４５％），センター

内，又はセンター以外の企業内端末からのアクセス（共に42%）であり，いずれも内部犯のケースである。これに対して，外部犯による探知型のケースは，企業外端末からのアクセス（22%），通信回線からの盗聴（28%），電波の傍受（14%）で，内部犯に比べると比率は低い。しかし相対的に比率が低いとはいえ，ハッカー等による探知型の情報犯罪の脅威を意識している企業が，回答者の2～3割に達していることは注目される。

企業規模別の特徴として，金融機関以外では，企業外端末からのアクセスに対する脅威の意識が，大企業に高く，中規模企業に低いという傾向がみられること（表－1，77ページ），金融機関の場合は，中小規模のクラスで，センター内でのアクセスの脅威が比較的高いこと（表－2，78ページ）が挙げられる。

1.2.2 情報の不正入手に関するセキュリティ対策 （アンケート 問3）

(1) 質問内容は，情報の不正入手を防止するため，企業が現実にどのようなセキュリティ対策を実施しているか，該当するもののすべてにレ印をつけるよう求めている（1.3問3，72ページ）。

実施企業の回答者全体に対する割合が最も高く60%台又は50%台に達しているのは，ルールの制定や取扱者の限定など，抽象的あるいは組織的な性格を有する措置である。すなわちルールの制定では，媒体管理66%，パスワード管理54%，重要出力情報管理52%，取扱者については，オペレーター専任制53%，重要情報入力取扱者の限定51%となっている。なお以上のほか多いものとしては，識別コード等による端末の確認62%，媒体の保管庫設置54%がある。

これに対して具体的に行動を規制したり，記録を義務づけることを内容とする措置になると，基本的なものでも実施企業の割合は40%台又は30%台となる。例えばパスワードによる本人確認47%，重要情報へのアクセス権限の定め48%，媒体保管室の入退管理44%，オペレーション記録の義務づけ39%，オペレーターの複数制35%，重要出力情報の担当責任者への直接引渡し35%等である。

行動のチェックを内容とする措置で，やや念の入ったものになると，

実施企業の割合は２０％台以下となる。例えば，重要情報の廃棄について責任者の立合い２９％，重要な出力情報の複写の承認２６％，入出力記録の検証２６％，重要情報の媒体の出し入れについて，管理台帳によるチェック２４％，パスワードの定期的変更２２％，端末室の入退管理１４％等である。

(2) （２．１）業種別では，金融業が他の業種に比べて，全般的にセキュリティ対策の実施率が高い（表－３～７，７９～８２ページ）。特に格差が大きいのは，具体的な行動規制や記録の義務づけ・検証である。例えばオフライン情報の媒体に関する，保管室の入退管理・管理台帳・廃棄のチェック，ＩＤコード等による本人確認，オペレーターの複数制及び責任者設置，コンソール・ログ，オペレーション記録の検証等である。なお，伝送情報の暗号化は，金融以外の業種には殆どみられないが，金融業の場合は，慣用鍵によるものが２割強みられる。

流通業と製造業の比較では，オンライン情報に関するアクセス，コントロールの面で，製造業の方が多少実施率が高いが，そのほかの分野では大差ないようである。

（２．２）規模別では，次のような傾向がみられる。

預金残高規模別（金融業）では，預金残高１兆円超とそれ以下でセキュリティ対策の実施率に格差がみられる（表－１３～１７，８５～８８ページ）。

年商規模別（金融業以外）及び従業員規模別では，共に，かなり多数の項目で中規模層にセキュリティ対策の実施率の落ち込みがみられるが，それ以上の規模では，規模が大きくなるにしたがって実施率も高まっている（表8～12，18～２２，８２～８５，８８～９１ページ）。

典型的な例は次のとおりである。

規模 ＼ セキュリティ対策	年商				従業員数			
	10億円超 100億円以下	100～1,000	1,000～5,000	5,000超	300人以下	300超 1,000以下	1,000～5,000	5,000超
・媒体保管室の入退管理	43％	26％	40％	100％	47％	29％	49％	78％
・パスワード等による本人確認	43	31	53	78	41	35	54	81
・オペレーター複数制	36	23	35	67	33	24	45	56
（回答者数）	47	120	40	9	70	102	94	27

以上のように年商100億円超1,000億円以下，従業員数300人超1,000人以下の層で実施率の落ち込みがみられる理由としては，経営的な余力に乏しくコスト面のプレッシャがきびしいという事情が推察されるが，それ以下の層で実施率が若干高いのは，この層に属する回答者は比較的電算装備率の高い特殊な企業であるためではないかと思われる。そこでこの層を特殊ケースとして除外すると，概ね規模にスライドしてセキュリティ対策の実施率が高まっているといえる。そのような相関関係は，コンピュータ投資規模別にみた場合一層明瞭である（表－23～27，91～94ページ）。それはセキュリティ対策が，コンピュータ投資に随伴して，ないしはその一環として行われる傾向があるためであろう。

以上のように企業規模や投資規模が大きくなるのに伴い，セキュリティ対策の実施率が高まっており，その理由はセキュリティ対策のコスト負担に耐える経営力の差異によるものと考えられる。

1.2.3 重要な情報の内容（アンケート問4）

重要な情報として特別のセキュリティ対策を講じている情報，又は特別のセキュリティ対策を講じているわけではないが，不正入手の潜在的脅威を強く意識している重要な情報として多く挙げられているものは，データの形態では，人事（回答者の49%），顧客リスト（35%）で，収支，資産・負債，原価計算，販売管理，顧客の信用情報がこれにつづいている（いずれも20%台，1.3問4，74ページ）。

なお製品開発・製造技術を挙げた者は，製造業に属する回答者（137社）に対する割合で示すと，データの形態で26%，プログラムの形態で18%である（1.3前文，69ページ，表30，96ページ）。

規模別にみると，殆どの項目について，重要情報を挙げている者の割合は，規模が大きくなるほど高くなっているが，その傾斜がゆるやかなものと，著しいものがある。人事，顧客リスト，販売，仕入れ，収支，原価計算などは，中小規模層でも重要情報として挙げている者の割合は相当程度あるので規模別の傾斜はゆるやかである。これに反して，資金移動，貸借，投資，不動産などに関する情報は．その性質上情報の重要性ないし秘密性を意識している者の割合は，大規模層にシフトしている

（表３１．３２，９７．９８ページ）。

1.2.4 セキュリティ対策の効果と隘路（アンケート問５）

(1) セキュリティ対策に相当の費用をかけた場合，その効果として，どのようなものが期待されるかという問に対しては（複数回答），「不正行為を安易に行えないようにする。」，「不正行為に対する倫理感や防犯意識を高める。」，「プロによる犯行や内部の計画的犯行を除いては，かなりの抑止効果が期待できる。」という回答がそれぞれ回答者の５割前後ある（５３％，４６％，４５％）（1.3問5.1，７５ページ）。

これらは，「でき心」や「遊び」で情報を覗きみるなど比較的軽い性質の不正行為の抑止にセキュリティ対策の主要な意義があるという理解が多いためではないかと思われる。実質的な情報犯罪に関しては，回答者の２５％が外部犯に対してある程度の抑止効果が期待できると答えている。

(2) セキュリティ対策の隘路に関し，どのようなものが重要視されるか（３つ以内で複数回答可）という質問に対し，セキュリティ対策の実施上の隘路としては，費用負担が大きい（回答者の７０％），重要情報に対するアクセス権限の細分化により仕事がやり難くなる（４６％）という点を指摘する声が多く，またセキュリティ対策の効果に関連する隘路として，内部の計画的犯行に対して有効なセキュリティ対策がないことを指摘する者が５８％に達している（1.3問5.2，７５ページ）。

コンピュータ・システムへの投資規模別にみると，費用負担を挙げる者の割合は，各クラス共高水準であるが，特に１０億円超５０億円以下のクラスでは回答者の約８０％と高く，このクラスはセキュリティ対策の実施割合も総体的に高い。一方投資額５千万円以下の小規模層では，セキュリティ対策の実施割合がかなり低いが，費用負担を隘路として挙げる者は回答者の６３％に達している。そのほか仕事がやり難くなるという点では，大規模層でアクセス権限の細分化や暗号化を挙げる者の割合が高くなっている（表３５，１０１ページ）。

1.2.5　企業秘密保持に関する定め（アンケート問6）

(1) 企業秘密の保持に関し，就業規則や従業員との間の契約で定めている企業は，回答者（289社）の84%で，定めのない企業は16%である。

定めのある場合，その形態は，就業規則によるものが回答者の81%，契約によるものが11%である（3.5%は就業規則と契約の両方で秘密保持の定めをしていることとなる）。

秘密保持の定めのある企業（241社）について，その定めの内容をみると，秘密保持を右職中のみ義務づけている者は67%，退職後も義務づけている者33%，保持すべき秘密の内容を抽象的に限定している者は40%，具体的に限定している者は2%（5社）である（1.3問6，75ページ）。

(2) 企業規模別にみると，金融以外の業種では，秘密保持の定めのない企業が，年商5,000億円超の大規模層と10億円以下の小規模層では皆無であるのに反し，10億円超5,000億円以下の中規模層で10～20%あるのが注目される（表36，102ページ）。

なお退職後も秘密保持を定めている者が小規模層で比較的多く，金融以外の業種では，年商10億円以下の層で55%（全体では29%），金融業では預金残高5,000億円以下の層で63%（全体では47%）となっている。コンピュータ・システムを保有しているような小規模企業の場合，従業員の転職による秘密漏洩が企業経営にダメージを与える危険性が強く意識されているものと思われる（表38，39，103ページ）。

1.2.6　情報の不正入手についての刑事立法に対する意見（アンケート問7）

(1) 情報の不正入手を刑事上の犯罪として処罰する立法について，基本的方向としてどのように考えるかというテーマで，3つの選択肢を選ばせる質問に対し，「①企業のセキュリティ対策で対処し得ない不正行為を抑止するため必要である。」という答えを選んだ者は33%，「②企業のセキュリティ対策を推進するうえで，不正行為の反社会性を立法によって明確化することが望ましい。」という答えを選んだ者は31%，「③刑事上の犯罪とすることについては，研究開発や従業員の転職の自由などを阻害するおそれもあるので，現行法で定められているもの（著作権，

通信の秘密による情報の保護等）以上に拡げることは望ましくない。契約責任や企業のセキュリティ対策によって対処することが望ましい。」という答えを選んだ者は38％である（①と②に多少の重複回答がある）（1.3問7，76ページ）。

先述のように（1.2.4－(2)），セキュリティ対策の盲路として，内部の計画的犯行に対しては有効なセキュリティ対策がないと答えをした者が回答者の58％あるが，これに対して刑事立法を必要とする者は33％にとどまっており，相当数が内部の計画的犯行に対してはセキュリティ対策が有効でないことを意識しながらも，それ以上に研究開発や従業員の転職の自由が損われるおそれへの配慮から，刑事立法に消極的な態度をとっているものと思われる。

(2) 企業規模別では，年商別の場合は，刑事立法に消極的な意見の割合が大規模ないし中規模上位層（1兆円超と1,000～5,000億円）及び小規模層（10億円以下）で多い。一方従業員数別の場合は，消極意見が中規模上位層（1,000～5,000人）に多く，大規模層のうち5,000～1万人で少なくなっている。また積極意見は大規模層（5,000人超）で多い。このように2つの表でちがった傾向がみられるので，規模別の特徴は余り明確ではないが，2つの表の共通点として中規模上位層（年商1,000～5,000億円，従業員数1,000～5,000人）で不要とする意見が多くなっている（51％，45％）。この層の企業については，市場での競争が激しく，情報の収集や人材の移動が比較的活発であるというような背景が作用しているのではないかとも考えられる（表40，41，104ページ）。

(3) 次に従業員数規模別による，セキュリティ対策の実施割合（表18～22，88～91ページ）と，刑事立法に対する意見（表41，104ページ）を対比してみると，セキュリティ対策の実施割合の特に大きい大規模層で積極意見が多い。それは2つの方向に現われており，セキュリティ対策で対処し得ない不正行為を阻止するため必要とする意見が5,000～1万人及び1万人超のクラスで共に多く（47％，44％），またセキュリティ対策を推進するうえで必要とする意見が5,000～1万人クラスで多くなっている（47％）。このクラスでは不要とする意見が特に少ない（18％）。

このような傾向がみられるのは，セキュリティ対策の実施割合の高い大規模層ほど，不正行為に対する防衛意識が高く，その場合セキュリティ対策と刑事立法は，一方があれば他方は不要視されるのではなく，協調・補完関係にあると考えられているためであろう。

セキュリティ対策の実施割合が低い小規模層では，刑事立法に対する意見は，大体全体平均なみに分散して特徴がない。セキュリティ対策の実施割合が中位である中規模上位層で(1,000～5,000人)刑事立法を不要とする意見が最も多いが(45%)，これは，この層の企業がおかれている前述の状況によるものであろう。

1.3　情報犯罪の脅威とセキュリティ対策等に関する調査

コンピュータ又はこれと結合した通信のシステムにおいて，保存，処理又は伝送される情報が不正に入手又は漏示される脅威と，これを防止するためのセキュリティ対策等についての質問及び回答の状況。（回答は，調査票に記載された選択肢にレをつける方法で行われた。）

回答集計数
- 金　融　36
- 流通業　27
- 製造業　137
- その他　97
- （合　計　297）

問1.　回答企業の概要及びコンピュータ・システムの状況について

1.1　年間売上高（金融機関の場合は預金残高）

（売上高）		（預金残高）	
①　10億円以下	12件	①　5,000億円以下	10件
②　10億円超～100億円以下	47	②　5,000億円超～1兆円以下	6
③　100億円超～1,000億円以下	120	③　1兆円超～5兆円以下	3
④　1,000億円超～5,000億円以下	40	④　5兆円超～10兆円以下	0
⑤　5,000億円超～1兆円以下	2	⑤　10兆円超	2
⑥　1兆円超	7		（計 21件）
（計 228件）			

1.2　従業員数（常勤）

①　300人以下	70件
②　300人超～1,000人以下	102
③　1,000人超～5,000人以下	94
④　5,000人超～1万人以下	17
⑤　1万人超	10
（計 293件）	

（コンピュータ・システムの状況）

1.3　コンピュータ・システムの導入時期

①	昭和60年以後	0件	③	昭和50年～54年	39
②	昭和55年～59年	6	④	昭和49年以前	251

（計 296件）

1.4　コンピュータ・システムへの投資規模（レンタルの場合は売価換算）

①	5,000万円以下	21	⑤	30億円超～50億円以下	15
②	5,000万円超～1億円以下	37	⑥	50億円超～100億円以下	7
③	1億円超～10億円以下	153	⑦	100億円超	11
④	10億円超～30億円以下	44			

（計 288件）

1.5　コンピュータに接続されている端末機の数

①	10以下	27	④	100超～500以下	72
②	10超～50以下	115	⑤	500超	28
③	50超～100以下	52			

（計 294件）

1.6　コンピュータに接続されている端末機の設置場所

①	自社内のみ	159	②	自社内及び自社外	137

（計 296件）

1.7　コンピュータの専任従業者における正社員の割合

①	50%以下	79（26.9%）	③	80%超	51（17.4%）
②	50%超～80%以下	44（15.0%）	④	100%	120（40.8%）

（計 294件）（100.0%）

1.8　コンピュータの業務内容（複数回答）

①	企画・調整	74	⑥	設計研究開発	87
②	購買	180	⑦	人事・給与	275
③	生産	144	⑧	資金・財務	228
④	販売	213	⑨	預貯金	134
⑤	製品在庫管理	190	⑩	その他	116

問 2. 情報の不正入手，不正漏示が行われる潜在的脅威について

2.1 潜在的脅威の程度

潜在的脅威の態様		潜在的脅威の程度			
		大	中	小	計
A 保存されている情報	①保管中又は移動時における媒体の持出し，複写等	49 (17.0)	82 (28.5)	157 (54.5)	288 (100.0)%
	②端末からのアクセスによるプリントアウト，盗視，複写等				
	②－1 センター内でのアクセス	37 (13.3)	79 (28.5)	161 (58.1)	277 (100.0)
	②－2 センター以外の企業内端末からのアクセス	26 (9.9)	85 (32.3)	152 (57.8)	263 (100.0)
	②－3 企業外端末からのアクセス	19 (8.0)	34 (14.4)	184 (77.6)	237 (100.0)
B システムの運用処理に係る情報	次の作業段階におけるプリントアウト，盗視，複写，媒体持出し等				
	① インプット	21 (7.7)	78 (28.6)	174 (63.7)	273 (100.0)
	② アウトプット	64 (22.2)	97 (33.7)	72 (44.1)	288 (100.0)
	③ オペレーション	28 (10.2)	72 (26.4)	173 (63.4)	273 (100.0)
	④ 委託処理	29 (13.6)	49 (23.0)	135 (63.4)	213 (100.0)
	⑤ その他〔 〕	0 (－)	1 (4.8)	20 (95.2)	21 (100.0)
C 伝送されている情報	①通信回線からの盗聴	14 (5.4)	58 (22.5)	186 (72.1)	258 (100.0)
	②電波の傍受	6 (2.6)	25 (10.9)	198 (86.5)	229 (100.0)

問3. 情報の不正入手，不正漏示に対するセキュリティ対策

3.1 保存情報（オフ・ライン）の管理

① 媒体保管の管理についてルールを定める。 197／297（66.3%）

② 保管室を定め，入退管理を行う。 131／297（44.1%）

③ 重要な情報については他と区別して施錠可能な保管庫に収納する。160／297（53.9%）

④ 管理責任者を定める。 187／297（63.0%）

⑤ 重要な情報について管理台帳を設け，管理者が出し入れをチェックする。71／297(23.9%)

⑥ 重要な情報の廃棄について管理責任者が立会う。 87／297（29.3%）

⑦ データベースのデータ更新に際しルールを定め，重要な情報について管理者がチェックする。 66／297（22.2%）

3.2 保存情報（オン・ライン）の管理

① 識別コード等により端末確認を行う。 183／297（61.6%）

② ＩＤカード，パスワード等により本人確認を行う。 140／297（47.1%）

③ 重要な情報についてのアクセス権限を定め，パスワードによりチェックする。 142／297（47.8%）

④ 重要な情報についてのアクセス権限を定め，プログラムとパスワードによりチェックする。 111／297（37.4%）

⑤ 重要な情報を暗号化する。 15／297（5.1%）

⑥ コンソール・ログ，システム使用状況記録等を検証し異常なアクセスをチェックする。 76／297（25.6%）

3.3 パスワード及び端末の管理

① パスワードの管理についてルールを定める。 160／297（53.9%）

② パスワードを記載した媒体の取扱者を限定する。 113／297（38.1%）

③ パスワードを定期的に変更する。 64／297（21.6%）

④ 異動時におけるパスワード廃棄のルールを定める。 47／297（15.8%）

⑤ パスワード発行は直接本人に対して行う。 88／297（29.6%）

⑥ パスワード管理部門をオペレーション部門から独立させる。 50／297（16.8%）

⑦ ＩＤカードにより端末室への入退管理を行う。　41／297（13.8％）

⑧ 端末室の管理責任者を定める。　55／297（18.5％）

⑨ 端末室への入退監視者（ガードマンなど）を任命する。　7／297（2.4％）

⑩ 端末室への入退についてＴＶカメラ等の監視装置を設ける。　14／297（4.7％）

3.4 処理情報の管理

（入力管理）

① 重要情報の入力について，取扱者を限定する。　152／297（51.2％）

② 入力される重要情報の原資料や，入力媒体の受渡し，保管等についてルールを定める。　134／297（45.1％）

（オペレーション管理）

③ オペレーターを専任制にする。　158／297（53.2％）

④ オペレーターを相互牽制の観点から複数制にする。　105／297（35.4％）

⑤ オペレーターの配置について責任者がコントールする。　91／297（30.6％）

⑥ オペレーション実施記録を検証する。　116／297（39.1％）

⑦ 重要情報の消去について確認する。　71／297（23.9％）

（出力管理）

⑧ 重要情報の保管のルールを定める。　152／297（51.2％）

⑨ 重要情報の複写について管理責任者の承認を要するものとする。　77／297（25.9％）

⑩ 重要情報の複写について特定のオペレーターの鍵を要するものとする。9／297（3.0％）

⑪ 重要情報について複数オペレーターにより相互チェックをさせる。　32／297（10.8％）

⑫ 重要情報の引渡しに際しては，担当責任者に直接渡すことを義務づける。　105／297（35.4％）

⑬ 重要情報の配付記録を設ける。　88／297（29.6％）

⑭ 重要情報の廃棄のルールを定める。　92／297（31.0％）

3.5 伝送情報の管理

① 重要情報の暗号化（慣用鍵）　19／297（6.4％）

② 重要情報の暗号化（公開鍵）　5／297（1.7％）

問 4. 重要な情報として特別のセキュリティ対策を講じている情報，又は特別のセキュリティ対策を講じているわけではないが不正入手，不正漏示の潜在的脅威を強く意識している重要な情報

重要な情報の形態 / 重要な情報の含まれる領域	(A) プログラム	(B) データベース	(C) データ
①製品開発，製造技術	24	29	35
②販売（貸付），仕入（預金）			
②－1 受発注	15	43	52
②－2 販売（貸付）管理	29	65	77
②－3 仕入（預金）管理	23	43	61
②－4 外注管理	10	14	25
②－5 在庫管理	16	32	45
③顧客（個人）			
③－1 顧客の信用情報	22	52	66
③－2 顧客リスト	28	71	102
③－3 顧客の暗証番号	17	22	38
③－4 その他	1	1	3
④需要予測	5	13	22
⑤事業計画	5	15	23
⑥企業財務			
⑥－1 収支	18	36	81
⑥－2 資産・負債	19	39	80
⑥－3 原価計算	22	44	81
⑥－4 その他	2	4	10
⑦資金			
⑦－1 大口の資金移動	12	16	44
⑦－2 貸借	13	18	41
⑦－3 投資	8	13	33
⑦－4 その他	0	0	2
⑧設備	4	7	13
⑨不動産	5	8	13
⑩株主	8	10	22
⑪人事	55	95	147
⑫コンピュータ・システム			
⑫－1 パスワード，暗号鍵等	49	41	69
⑫－2 その他	7	2	6
⑬その他	3	11	11

（回答企業数 297）

問 5. 情報の不正入手，不正漏示に向けられたセキュリティ対策の抑止効果について

5.1 セキュリティ対策に相当の費用をかけた場合の効果

（ 2つ以内複数回答可能 ）

① 不正行為を安易に行えないようにする。 142／267（53.2%）

② 不正行為に対する倫理感や防犯意識を高める。 122／267（45.7%）

③ 外部犯に対してはある程度の抑止効果がある。 66／267（24.7%）

④ プロによる犯行や，内部の計画的犯行を除いては，かなりの抑止効果が期待できる。

121／267（45.3%）

5.2 セキュリティ対策の隘路

（ 3つ以内複数回答可能 ）

① 費用の負担が大きい。 176／253（69.6%）

② 次の規制を強めると，仕事がやり難くなる。

②－1 重要情報に対するアクセス権限の細分化 117／253（46.3%）

②－2 重要情報の暗号化 55／253（21.7%）

②－3 複数オペレーターによる相互チェック 43／253（17.0%）

②－4 媒体の受渡しのチェック 32／253（12.7%）

②－5 入退室のチェック 45／253（17.8%）

②－6 その他〔 〕 1／253（0.4%）

③ パスワードの管理が難しい。 31／253（12.3%）

④ 内部の計画的犯行に対して有効なセキュリティ対策がない。 146／253（57.7%）

⑤ その他 4／253（1.6%）

問 6. 企業秘密の取扱い

6.1 貴社では，就業規則や従業員との間の契約で，企業秘密の保持に関し定めていますか。

① 就業規則で定めている。 233／289（80.6%）

② 契約で定めている。 31／289（10.7%）

③ 定めていない。 46／289（15.9%）

6.2　上記 6.1 の①又は②に該当する場合の内容

① 在職中のみ秘密保持を義務づけている。　162／241（67.2%）

② 退職後も秘密保持を義務づけている。　79／241（32.8%）

③ 退職後に，競合的なシステムや類似のシステムの開発に携わることを禁じている。

2／241（0.8%）

④ 退職後の義務や禁止については期間を限定している。　4／241（1.7%）

⑤ 保持すべき秘密の内容を抽象的に限定している。　96／241（39.8%）

⑥ 保持すべき秘密の内容を具体的に限定している。　5／241（2.1%）

⑦ その他　5／241（2.1%）

問7. 情報の不正入手，不正漏示を刑事上の犯罪として処罰する立法について

① 企業のセキュリティ対策で対処し得ない不正行為を抑止するため必要である。

91／275（33.1%）

② 企業のセキュリティ対策を推進するうえで，不正行為の反社会性を立法によって明確化することが望ましい。　86／275（31.3%）

③ 刑事法上の「犯罪」とすることについては，研究開発や従業員の転職の自由などを阻害するおそれもあるので，現行法で定められているもの（著作権，通信の秘密による情報の保護等）以上に拡げることは望ましくない。契約責任や企業のセキュリティ対策によって対処することが望ましい。　104／275（37.8%）

④ その他　3／275（1.1%）

2. 層別集計表

ここに掲げた「層別集計表」は，アンケート各項目の集計値の相互関連について，「x^2」計算による不相関（独立性）の検定を行った結果，相関関係の検出されたデータ（x^2 値1％以内）から，主要なものを選んで配列した表である。

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－1）

〔横の問〕　1.2　年間売上高

〔縦の問〕　2.1　潜在的脅威の程度をどのように意識していますか。（潜在的脅威の程度　大＋中　　）

（単位％）　　（金融機関以外）

項　目	①10以下	②10～	③100	④1000	⑤5000	⑥1兆	合　計
A① 保管移動	60.00	50.00	44.28	50.00	100.00	60.00	48.18
A②—1センタ内	20.00	38.46	45.71	46.66	100.00	40.00	43.80
A②—2センタ外	60.00	50.00	45.71	40.00	100.00	40.00	45.99
A②—3企業外	40.00	15.38	18.57	13.33	100.00	60.00	19.71
B① イ　ン	20.00	38.46	37.14	30.00	100.00	60.00	36.50
B② アウト	60.00	61.54	58.57	63.34	100.00	60.00	60.59
B③ オ　ペ	40.00	46.16	34.28	46.66	100.00	60.00	40.88
B④ 委託処理	60.00	26.92	34.28	40.00	100.00	80.00	32.12
B⑤ その他	0.00	0.00	1.43	0.00	0.00	0.00	0.73
C① 盗　聴	20.00	23.08	25.71	30.00	100.00	20.00	26.28
C② 傍　受	0.00	11.54	15.72	13.33	100.00	0.00	13.87
各層のケース数	100.00	100.00	100.00	100.00	100.00	100.00	100.00
度　数	5	26	70	30	1	5	137

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－２）

〔横の問〕　1.2　預金残高

〔縦の問〕　2.1　潜在的脅威の程度をどのように意識していますか。（潜在的脅威の程度　大＋中　　）

（単位：％）　　（金融機関）

項　目	①5千以下	②5000～	③1兆	④5兆	⑤10兆	合 計
A① 保管移動	50.00	75.00	0.00	0.00	0.00	46.67
A②－1 センタ内	75.00	25.00	100.00	0.00	0.00	53.33
A②－2 センタ外	25.00	25.00	100.00	0.00	0.00	26.67
A②－3 企業外	12.50	25.00	0.00	0.00	0.00	13.34
B① イ　ン	25.00	25.00	100.00	0.00	50.00	33.33
B② アウト	37.50	25.00	100.00	0.00	50.00	40.00
B③ オ　ペ	37.50	25.00	100.00	0.00	50.00	40.00
B④ 委託処理	37.50	50.00	0.00	0.00	50.00	40.00
B⑤ その他	0.00	0.00	0.00	0.00	0.00	0.00
C① 盗　聴	12.50	50.00	100.00	0.00	0.00	26.67
C② 傍　受	12.50	0.00	100.00	0.00	0.00	13.33
各層のケース数	100.00	100.00	100.00	0.00	100.00	100.00
回 答 数	8	4	1	0	2	15

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－3）

〔横の問〕　1.0　業種

〔縦の問〕　3.1　保存情報（オフ・ライン）の管理

（単位：％）

項　目	①金融業	②流通業	③製造業	④その他	合　計
①　ル　ー　ル	80.56	66.67	61.31	68.04	66.33
②　入退管理	72.22	29.63	30.66	56.70	44.11
③　保　管　庫	75.00	37.04	43.80	64.95	53.87
④　責　任　者	77.78	62.96	59.85	61.86	62.96
⑤　管理台帳	47.22	14.81	11.68	35.05	23.91
⑥　廃　　棄	52.78	18.52	20.44	36.08	29.29
⑦　更　　新	47.22	25.93	15.33	21.65	22.22
各層のケース数	100.00	100.00	100.00	100.00	100.00
度　　数	36	27	137	97	297

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－4）

〔横の問〕　1.0　業種

〔縦の問〕　3.2　保存情報（オン・ライン）の管理

（単位：％）

項　目	①金融業	②流通業	③製造業	④その他	合　計
①　コード等	72.22	51.85	62.04	59.79	61.62
②　I　　D	69.44	22.22	39.42	56.70	47.14
③　パ　　ス	36.11	29.63	49.64	54.64	47.81
④　プロ，パス	52.78	22.22	32.12	43.30	37.37
⑤　暗　号　化	11.11	3.70	3.65	5.15	5.05
⑥　検　　証	69.44	11.11	16.79	25.77	25.59
各層のケース数	100.00	100.00	100.00	100.00	100.00
度　　数	36	27	137	97	297

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－5）

〔横の問〕　1.0　業種

〔縦の問〕　3.3　パスワード及び端末の管理

（単位：％）

項　目	①金融業	②流通業	③製造業	④その他	合　計
①　ル　ー　ル	52.78	48.15	54.74	54.64	53.87
②　限　　定	55.56	29.63	27.74	48.45	38.05
③　定　期　的	25.00	7.41	16.06	31.96	21.55
④　異　動　時	36.11	14.81	8.76	18.56	15.82
⑤　直接本人	36.11	14.81	26.28	36.08	29.63
⑥　独　　立	25.00	11.11	10.95	23.71	16.84
⑦　入退管理	38.89	3.70	6.57	17.53	13.80
⑧　責　任　者	22.22	7.41	15.33	24.74	18.52
⑨　監　視　者	8.33	0.00	0.73	3.09	2.36
⑩　監視装置	22.22	0.00	2.19	3.09	4.71
各層のケース数	100.00	100.00	100.00	100.00	100.00
度　　数	36	27	137	97	297

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－6）

〔横の問〕　1.0　業種

〔縦の問〕　3.4　処理情報の管理

（単位：％）

項　目	①金融業	②流通業	③製造業	④その他	合　計
①　人限定	47.22	48.15	58.39	43.30	51.18
②　人ルール	61.11	37.04	36.50	53.61	45.12
③　オ専任制	52.78	51.85	51.82	55.67	53.20
④　オ複数制	61.11	29.63	26.28	40.21	35.35
⑤　オ責任者	50.00	25.93	24.09	34.02	30.64
⑥　オ記録	63.89	29.63	29.20	46.39	39.06
⑦　オ消去	33.33	25.93	18.98	26.80	23.91
⑧　出ルール	61.11	48.15	46.72	54.64	51.18
⑨　出承認	36.11	29.63	17.52	32.99	25.93
⑩　出　鍵	13.89	0.00	0.73	3.09	3.03
⑪　出相互	33.33	7.41	3.65	13.40	10.77
⑫　出直接	41.67	37.04	33.58	35.05	35.35
⑬　出記録	47.22	22.22	23.36	34.02	29.63
⑭　出廃棄	38.89	25.93	27.74	34.02	30.98
各層のケース数	100.00	100.00	100.00	100.00	100.00
度　数	36	27	137	97	297

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－7）

〔横の問〕　1.0　業種

〔縦の問〕　3.5　伝送情報の管理

（単位：％）

項　目	①金融業	②流通業	③製造業	④その他	合　計
①　慣用鍵	22.22	3.70	2.92	6.19	6.40
②　公開鍵	2.78	7.41	0.73	1.03	1.68
各層のケース数	100.00	100.00	100.00	100.00	100.00
度　数	36	27	137	97	297

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－8）

〔横の問〕　1.2　年間売上高

〔縦の問〕　3.1　保存情報（オフ・ライン）の管理

（単位：％）　　（金融機関以外）

項　目	①10以下	②10～	③100	④1000	⑤5000	⑥1兆	合　計
①　ルール	58.33	59.57	59.17	82.50	50.00	100.00	64.47
②　人退管理	83.33	42.55	25.83	40.00	100.00	100.00	37.72
③　保管庫	100.00	44.68	43.33	55.00	100.00	71.43	50.00
④　責任者	83.33	68.09	52.50	60.00	100.00	85.71	60.09
⑤　管理台帳	33.33	27.66	13.33	15.00	50.00	42.86	18.86
⑥　廃　棄	33.33	29.79	25.00	22.50	0.00	28.57	25.88
⑦　更　新	16.67	23.40	18.33	15.00	0.00	28.57	18.86
各層のケース数	100.00	100.00	100.00	100.00	100.00	100.00	100.00
度　数	12	47	120	40	2	7	228

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－9）

〔横の問〕　1.2　年間売上高

〔縦の問〕　3.2　保存情報（オン・ライン）の管理

（単位：％）　　（金融機関以外）

項　目	①10以下	②10～	③100	④1000	⑤5000	⑥1兆	合　計
①　コード等	58.33	57.45	55.83	70.00	100.00	85.71	60.09
②　I　D	41.67	42.55	30.83	52.50	100.00	71.43	39.47
③　パ　ス	41.67	53.19	42.50	57.50	100.00	71.43	48.68
④　プロ，パス	41.67	38.30	27.50	25.00	100.00	85.71	32.46
⑤　暗号化	8.33	4.26	0.83	12.50	0.00	28.57	4.82
⑥　検　証	16.67	17.02	17.50	15.00	50.00	42.86	17.98
各層のケース数	100.00	100.00	100.00	100.00	100.00	100.00	100.00
度　数	12	47	120	40	2	7	228

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－10）

〔横の問〕　1.2　年間売上高

〔縦の問〕　3.3　パスワード及び端末の管理

（単位：％）　　（金融機関以外）

項　目	①10以下	②10～	③100	④1000	⑤5000	⑥1兆	合　計
①　ル　ー　ル	58.33	48.94	45.83	67.50	50.00	85.71	52.19
②　限　定	50.00	36.17	29.17	35.00	100.00	57.14	34.21
③　定期的	25.00	31.91	14.17	17.50	50.00	28.57	19.74
④　異動時	16.67	8.51	9.17	17.50	50.00	28.57	11.84
⑤　直接本人	50.00	36.17	20.00	27.50	100.00	57.14	28.07
⑥　独　立	8.33	19.15	13.33	12.50	0.00	28.57	14.47
⑦　人退管理	25.00	8.51	5.00	10.00	100.00	57.14	10.09
⑧　責任者	33.33	23.40	15.83	15.00	0.00	28.57	18.42
⑨　監視者	0.00	2.13	0.00	2.50	0.00	14.29	1.32
⑩　監視装置	0.00	2.13	0.83	5.00	0.00	14.29	2.19
各層のケース数	100.00	100.00	100.00	100.00	100.00	100.00	100.00
度　数	12	47	120	40	2	7	228

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－11）

〔横の問〕　1.2　年間売上高

〔縦の問〕　3.4　処理情報の管理

（単位：％）　　（金融機関以外）

項　目	① 10以下	② 10～	③ 100	④ 1000	⑤ 5000	⑥ 1兆	合　計
①　人限定	33.33	51.06	54.17	57.50	50.00	42.86	52.63
②　人ルール	33.33	42.55	38.33	42.50	100.00	71.43	41.23
③　オ専任制	58.33	46.81	50.00	60.00	100.00	100.00	53.51
④　オ複数制	41.67	36.17	22.50	35.00	50.00	71.43	30.26
⑤　オ責任者	33.33	27.66	20.83	40.00	100.00	42.86	27.63
⑥　オ記録	33.33	27.66	28.33	45.00	100.00	85.71	33.77
⑦　オ消去	25.00	34.04	17.50	35.00	0.00	42.86	25.00
⑧　出ルール	50.00	44.68	47.50	57.50	100.00	85.71	50.44
⑨　出承認	33.33	19.15	21.67	30.00	0.00	57.14	24.12
⑩　出鍵	8.33	4.26	0.00	0.00	0.00	14.29	1.75
⑪　出相互	25.00	10.64	1.67	12.50	0.00	0.00	6.58
⑫　出直後	41.67	25.53	33.33	35.00	50.00	71.43	33.77
⑬　出記録	41.67	27.66	22.50	27.50	0.00	42.86	25.88
⑭　出廃棄	41.67	34.04	24.17	30.00	50.00	85.71	30.26
各層のケース数	100.00	100.00	100.00	100.00	100.00	100.00	100.00
度　数	12	47	120	40	2	7	228

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－12）

〔横の問〕　1.2　年間売上高

〔縦の問〕　3.5　伝送情報の管理

（単位：％）　　（金融機関以外）

項　目	①10以下	②10～	③100	④1000	⑤5000	⑥1兆	合　計
①　慣用鍵	8.33	4.26	2.50	2.50	0.00	14.29	3.51
②　公開鍵	0.00	0.00	1.67	0.00	0.00	14.29	1.32
各層のケース数	100.00	100.00	100.00	100.00	100.00	100.00	100.00
度　数	12	47	120	40	2	7	228

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－13）

〔横の問〕　1.2　預金残高

〔縦の問〕　3.1　保存情報（オフ・ライン）の管理

（単位：％）　　（金融機関）

項　目	①5千以下	②5000～	③1兆	④5兆	⑤10兆	合　計
①　ルール	100.00	83.33	100.00	0.00	100.00	95.24
②　入退管理	70.00	66.67	100.00	0.00	100.00	76.19
③　保管庫	70.00	100.00	100.00	0.00	100.00	85.71
④　責任者	80.00	66.67	100.00	0.00	100.00	80.95
⑤　管理台帳	40.00	66.67	100.00	0.00	100.00	61.90
⑥　廃　棄	70.00	50.00	100.00	0.00	100.00	71.43
⑦　更　新	40.00	66.67	100.00	0.00	100.00	61.90
各層のケース数	100.00	100.00	100.00	0.00	100.00	100.00
度　数	10	6	3	0	2	21

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－14）

〔横の問〕　1.2　預金残高

〔縦の問〕　3.2　保存情報（オン・ライン）の管理

（単位：％）　　（金融機関）

項　目	①5千以下	②5000～	③1兆	④5兆	⑤10兆	合　計
①　コード等	80.00	83.33	100.00	0.00	100.00	85.71
②　I　D	70.00	83.33	100.00	0.00	100.00	80.95
③　パ　ス	60.00	33.33	33.33	0.00	50.00	47.62
④　プロ，パス	40.00	66.67	100.00	0.00	100.00	61.90
⑤　暗号化	0.00	16.67	100.00	0.00	0.00	19.05
⑥　検　証	70.00	100.00	100.00	0.00	100.00	85.71
各層のケース数	100.00	100.00	100.00	0.00	100.00	100.00
度　数	10	6	3	0	2	21

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－15）

〔横の問〕　1.2　預金残高

〔縦の問〕　3.3　パスワード及び端末の管理

（単位：％）　　（金融機関）

項　目	①5千以下	②5000～	③1兆	④5兆	⑤10兆	合　計
①　ル　ー　ル	40.00	66.67	66.67	0.00	100.00	57.14
②　限　定	40.00	83.33	66.67	0.00	100.00	61.90
③　定期的	50.00	33.33	33.33	0.00	0.00	38.10
④　異動時	30.00	16.67	66.67	0.00	100.00	38.10
⑤　直接本人	50.00	33.33	66.67	0.00	50.00	47.62
⑥　独　立	20.00	33.33	66.67	0.00	100.00	38.10
⑦　人退管理	40.00	66.67	100.00	0.00	50.00	57.14
⑧　責任者	10.00	33.33	100.00	0.00	0.00	28.57
⑨　監視者	0.00	16.67	33.33	0.00	50.00	14.29
⑩　監視装置	10.00	50.00	100.00	0.00	50.00	38.10
各層のケース数	100.00	100.00	100.00	0.00	100.00	100.00
度　数	10	6	3	0	2	21

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－16）

〔横の問〕　1.2　預金残高

〔縦の問〕　3.4　処理情報の管理

（単位：%）　　（金融機関）

項　目	①5千以下	②5000～	③1兆	④5兆	⑤10兆	合　計
①人限定	40.00	33.33	66.67	0.00	100.00	47.62
②人ルール	70.00	83.33	100.00	0.00	100.00	80.95
③オ専任制	40.00	66.67	100.00	0.00	100.00	61.90
④オ複数制	40.00	100.00	100.00	0.00	50.00	66.67
⑤オ責任者	40.00	50.00	66.67	0.00	100.00	52.38
⑥オ記録	70.00	83.33	66.67	0.00	100.00	76.19
⑦オ消去	20.00	50.00	66.67	0.00	100.00	42.86
⑧出ルール	60.00	50.00	100.00	0.00	100.00	66.67
⑨出承認	10.00	50.00	100.00	0.00	100.00	42.86
⑩出鍵	10.00	0.00	0.00	0.00	50.00	9.52
⑪出相互	20.00	83.33	66.67	0.00	50.00	47.62
⑫出直接	40.00	50.00	66.67	0.00	100.00	52.38
⑬出記録	60.00	66.67	100.00	0.00	50.00	66.67
⑭出廃棄	50.00	33.33	100.00	0.00	100.00	57.14
各層のケース数	100.00	100.00	100.00	0.00	100.00	100.00
度　数	10	6	3	0	2	21

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－17）

〔横の問〕　1.2　預金残高

〔縦の問〕　3.5　伝送情報の管理

（単位：％）　　（金融機関）

項　　目	①5千以下	②5000～	③1兆	④5兆	⑤10兆	合　計
①慣用鍵	10.00	16.67	100.00	0.00	100.00	33.33
②公開鍵	0.00	0.00	33.33	0.00	0.00	4.76
各層のケース数	100.00	100.00	100.00	0.00	100.00	100.00
度　　数	10	6	3	0	2	21

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－18）

〔横の問〕　1.3　従業員数（常勤）

〔縦の問〕　3.1　保存情報（オフ・ライン）の管理

（単位：％）

項　　目	①3百以下	②300～	③1000	④5000	⑤1万	合　計
①ルール	61.43	57.84	72.34	88.24	100.00	66.55
②人退管理	47.14	29.41	48.94	76.47	80.00	44.37
③保管庫	48.57	40.20	68.09	70.59	70.00	53.92
④責任者	70.00	52.94	60.64	88.24	90.00	62.80
⑤管理台帳	27.14	14.71	23.40	41.18	60.00	23.55
⑥廃　　棄	27.14	26.47	31.91	41.18	40.00	29.69
⑦更　　新	24.29	19.61	20.21	29.41	40.00	22.18
各層のケース数	100.00	100.00	100.00	100.00	100.00	100.00
度　　数	70	102	94	17	10	293

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－19）

〔横の問〕　1.3　従業員数（常勤）

〔縦の問〕　3.2　保存情報（オン・ライン）の管理

（単位：％）

項　目	①3百以下	②300～	③1000	④5000	⑤1万	合　計
①　コード数	50.00	55.88	69.15	88.24	90.00	61.77
②　I　D	41.43	35.29	54.26	82.35	80.00	47.10
③　パ　ス	41.43	42.16	51.06	64.71	80.00	47.44
④　プロ，パス	32.86	27.45	44.68	52.94	90.00	37.88
⑤　暗　化	2.86	2.94	5.32	17.65	20.00	5.12
⑥　検　証	17.14	22.55	29.79	41.18	60.00	25.94
各層のケース数	100.00	100.00	100.00	100.00	100.00	100.00
度　数	70	102	94	17	10	293

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－20）

〔横の問〕　1.3　従業員数（常勤）

〔縦の問〕　3.3　パスワード及び端末の管理

（単位：％）

項　目	①3百以下	②300～	③1000	④5000	⑤1万	合　計
①　ル　ー　ル	41.43	47.06	61.70	94.12	80.00	54.27
②　限　定	42.86	23.53	39.36	70.59	80.00	37.88
③　定　期　的	17.14	17.65	23.40	58.82	20.00	21.84
④　異　動　時	14.29	12.75	15.96	35.29	30.00	16.04
⑤　直接本人	32.86	22.55	28.72	52.94	50.00	29.69
⑥　独　立	14.29	10.78	20.21	35.29	40.00	17.06
⑦　人退管理	10.00	7.84	17.02	29.41	50.00	13.99
⑧　責　任　者	20.00	17.65	20.21	17.65	10.00	18.77
⑨　監　視　者	1.43	0.00	2.13	11.76	20.00	2.39
⑩　監視装置	1.43	1.96	8.51	5.88	20.00	4.78
各層のケース数	100.00	100.00	100.00	100.00	100.00	100.00
度　数	70	102	94	17	10	293

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－21）

〔横の問〕　1.3　従業員数（常勤）

〔縦の問〕　3.4　処理情報の管理

（単位：％）

項　　目	①3百以下	②300～	③1000	④5000	⑤1万	合　計
①　入限定	50.00	52.94	48.94	52.94	60.00	51.19
②　入ルール	40.00	35.29	54.26	64.71	70.00	45.39
③　オ専任制	54.29	41.18	57.45	82.35	90.00	53.58
④　オ複数制	32.86	23.53	44.68	52.94	60.00	35.49
⑤　オ責任者	35.71	20.59	29.79	64.71	60.00	31.06
⑥　オ記録	32.86	27.45	47.87	70.59	80.00	39.59
⑦　オ消去	31.43	17.65	24.47	23.53	40.00	24.23
⑧　出ルール	50.00	45.10	54.26	64.71	70.00	51.19
⑨　出承認	25.71	20.59	27.66	29.41	60.00	25.94
⑩　出　鍵	8.57	0.00	1.06	0.00	20.00	3.07
⑪　出相互	14.29	5.88	12.77	17.65	10.00	10.92
⑫　出直接	30.00	29.41	41.49	52.94	60.00	35.84
⑬　出記録	31.43	17.65	37.23	58.82	30.00	30.03
⑭　出廃棄	30.00	21.57	37.23	35.29	70.00	31.06
各層のケース数	100.00	100.00	100.00	100.00	100.00	100.00
度　　数	70	102	94	17	10	293

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－22）

〔横の問〕　1.3　従業員数（常勤）

〔縦の問〕　3.5　伝送情報の管理

（単位：％）

項　　目	① 3百以下	② 300～	③ 1000	④ 5000	⑤ 1万	合　計
①　慣用鍵	4.29	1.96	7.45	17.65	30.00	6.14
②　公開鍵	0.00	0.98	3.19	5.88	0.00	1.71
各層のケース数	100.00	100.00	100.00	100.00	100.00	100.00
度　　数	70	102	94	17	10	293

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－23）

〔横の問〕　1.5　コンピュータ・システムへの投資規模（レンタルの場合は売価換算）

〔縦の問〕　3.1　保存情報（オフ・ライン）の管理

（単位：％）

項　　目	① 5千以下	②～ 5000	③ 1億	④ 10億	⑤ 30億	⑥ 50億	⑦ 100億	合　計
①　ルール	28.57	51.35	66.67	72.73	86.67	100.00	90.91	65.63
②　入退管理	23.81	18.92	39.87	59.09	66.67	85.71	81.82	43.06
③　保管庫	33.33	24.32	53.59	68.18	66.67	100.00	63.64	52.78
④　責任者	61.90	45.95	60.78	65.91	66.67	100.00	81.82	61.81
⑤　管理台帳	9.52	2.70	18.95	34.09	53.33	57.14	63.64	22.92
⑥　廃　棄	19.05	24.32	27.45	36.36	46.67	57.14	27.27	29.51
⑦　更　新	19.05	13.51	21.57	18.18	33.33	57.14	36.36	21.88
各層のケース数	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00
度　　数	21	37	153	44	15	7	11	288

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－24）

〔横の問〕　1.5　コンピュータ・システムへの投資規模（レンタルの場合は売価換算）

〔縦の問〕　3.2　保存情報（オン・ライン）の処理

（単位：％）

項　目	① 5千以下	②　～ 5000	③ 1億	④ 10億	⑤ 30億	⑥ 50億	⑦ 100億	合　計
①　コード等	23.81	43.24	63.40	75.00	73.33	57.14	72.73	60.42
②　I　D	28.57	18.92	41.18	72.73	73.33	100.00	72.73	46.53
③　パ　ス	28.57	29.73	47.71	56.82	80.00	42.86	45.45	46.88
④　プロ，パス	23.81	18.92	33.99	45.45	53.33	100.00	63.64	36.81
⑤　暗号化	0.00	2.70	1.96	11.36	13.33	28.57	18.18	5.21
⑥　検　証	9.52	8.11	22.22	40.91	40.00	57.14	54.55	25.35
各層のケース数	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00
度　数	21	37	153	44	15	7	11	288

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－25）

〔横の問〕　1.5　コンピュータ・システムへの投資規模（レンタルの場合は売価換算）

〔縦の問〕　3.3　パスワード及び端末の管理

（単位：％）

項　目	① 5千以下	②　～ 5000	③ 1億	④ 10億	⑤ 30億	⑥ 50億	⑦ 100億	合　計
①　ル　ー　ル	9.52	40.54	54.90	61.36	73.33	71.43	90.91	53.47
②　限　定	14.29	29.73	36.60	47.73	53.33	57.14	45.45	37.50
③　定期的	14.29	8.11	20.26	31.82	33.33	57.14	27.27	21.88
④　異動時	4.76	0.00	16.99	27.27	20.00	28.57	9.09	15.63
⑤　直接本人	19.05	18.92	26.14	38.64	53.33	42.86	36.36	28.82
⑥　独　立	14.29	8.11	12.42	27.27	13.33	71.43	36.36	16.67
⑦　入退管理	0.00	0.00	7.19	31.82	26.67	71.43	27.27	12.85
⑧　責任者	4.76	10.81	20.92	25.00	13.33	57.14	9.09	19.10
⑨　監視者	0.00	0.00	0.65	4.55	0.00	14.29	18.18	2.08
⑩　監視装置	0.00	0.00	1.31	15.91	6.67	28.57	9.09	4.51
各層のケース数	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00
度　数	21	37	153	44	15	7	11	288

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－26）

〔横の問〕　1.5　コンピュータ・システムへの投資規模（レンタルの場合は売価換算）

〔縦の問〕　3.4　処理情報の管理

（単位：%）

項　　目	① 5千以下	②　～ 5000	③ 1億	④ 10億	⑤ 30億	⑥ 50億	⑦ 100億	合　計
①　入限定	61.90	48.65	51.63	47.73	40.00	42.86	63.64	51.04
②　入ルール	19.05	24.32	43.14	59.09	86.67	71.43	63.64	45.14
③　オ専任制	33.33	43.24	47.06	72.73	60.00	100.00	72.73	52.43
④　オ複数制	14.29	18.92	30.72	59.09	66.67	71.43	45.45	35.76
⑤　オ責任者	14.29	5.41	29.41	50.00	40.00	57.14	45.45	30.21
⑥　オ記録	4.76	13.51	35.95	63.64	60.00	85.71	63.64	38.54
⑦　オ消去	19.05	21.62	22.88	29.55	20.00	14.29	45.45	23.96
⑧　出ルール	33.33	43.24	50.98	54.55	53.33	100.00	63.64	51.04
⑨　出承認	14.29	10.81	24.18	29.55	26.67	71.43	72.73	25.69
⑩　出　鍵	4.76	2.70	2.61	4.55	0.00	0.00	0.00	2.78
⑪　出相互	4.76	8.11	8.50	18.18	26.67	14.29	18.18	11.11
⑫　出直接	19.05	24.32	36.60	40.91	40.00	57.14	54.55	35.76
⑬　出記録	14.29	16.22	29.41	40.91	40.00	71.43	27.27	29.86
⑭　出廃棄	4.76	27.03	29.41	31.82	33.33	100.00	72.73	31.25
各層のケース数	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00
度　　数	21	37	153	44	15	7	11	288

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－27）

〔横の問〕　1.5　コンピュータ・システムへの投資規模（レンタルの場合は売価換算）

〔縦の問〕　3.5　伝送情報の管理

（単位：％）

項　　目	① 5千以下	②　～ 5000	③ 1億	④ 10億	⑤ 30億	⑥ 50億	⑦ 100億	合　計
①　慣用鍵	0.00	0.00	3.92	9.09	13.33	57.14	18.18	6.25
②　公開鍵	0.00	0.00	0.65	4.55	6.67	14.29	0.00	1.74
各層のケース数	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00
度　　数	21	37	153	44	15	7	11	288

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－28）

〔横の問〕　1.6　コンピュータに接続されている端末の数

〔縦の問〕　3.2　保存情報（オン・ライン）の管理

（単位：％）

項　目	①10以下	②10～	③50	④100	⑤500	合　計
①　コード等	40.74	47.83	71.15	75.00	89.29	61.90
②　I　D	22.22	40.00	38.46	59.72	85.71	47.28
③　パ　ス	22.22	44.35	53.85	56.94	53.57	47.96
④　プロ，パス	29.63	21.74	48.08	47.22	64.29	37.42
⑤　暗号化	3.70	0.87	5.77	5.56	21.43	5.10
⑥　検　証	3.70	14.78	32.69	37.50	46.43	25.51
各層のケース数	100.00	100.00	100.00	100.00	100.00	100.00
度　数	27	115	52	72	28	294

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－29）

〔横の問〕　1.7　コンピュータに接続されている端末機の設置場所

〔縦の問〕　3.2　保存情報（オン・ライン）の管理

（単位：％）

項　目	①自社内	②自社内外	合　計	項　目	①自社内	②自社内外	合　計
①　コード等	52.83	72.26	61.82	⑤　暗号化	2.52	8.03	5.07
②　I　D	38.36	57.66	47.30	⑥　検　証	20.13	32.12	25.68
③　パ　ス	43.40	53.28	47.97	各層のケース数	100.00	100.00	100.00
④プロ，パス	29.56	46.72	37.50	度　数	159	137	296

〔層別集計表（各層別ケース数に対する割合<層：横の問>）

（表－30）

〔横の問〕　1.0　業種

〔縦の問〕　4.　不正入手，不正漏示の潜在的脅威を強く意識している重要な情報としては，どのようなものがありますか。（複数回答）

（単位：％）

項　目	①金融業	②流通業	③製造業	④その他	合　計
①開発技術	0.00	0.00	32.03	11.83	18.77
②—1 受発注	6.45	28.00	42.97	9.68	26.35
②—2 販　売	41.94	56.00	46.88	24.73	39.71
②—3 仕入れ	41.94	32.00	37.50	12.90	29.24
②—4 外注管理	3.23	12.00	17.19	5.38	11.19
②—5 在庫管理	6.45	52.00	32.81	12.90	24.91
③—1 信用情報	77.42	40.00	21.88	27.96	31.77
③—2 リスト	58.06	52.00	41.41	44.09	45.13
③—3 暗証番号	80.65	12.00	5.47	9.68	15.88
③—4 顧その他	0.00	0.00	0.78	2.15	1.08
④需要予測	3.23	4.00	14.84	7.53	10.11
⑤事業計画	3.23	4.00	14.84	4.30	9.03
⑥—1 収　支	12.90	48.00	39.84	31.18	34.66
⑥—2 資産負債	16.13	36.00	42.97	30.11	35.02
⑥—3 原価計算	6.45	20.00	55.47	25.81	36.82
⑥—4 ⑥その他	0.00	8.00	3.91	5.38	4.33
⑦—1 資金移動	19.35	20.00	17.97	16.13	17.69
⑦—2 貸　借	22.58	24.00	17.97	13.98	17.69
⑦—3 投　資	9.68	20.00	13.28	11.83	13.00
⑦—4 ⑦その他	0.00	0.00	1.56	0.00	0.72
⑧設　備	3.23	8.00	8.59	3.23	6.14
⑨不動産	6.45	4.00	7.03	5.38	6.14
⑩株　主	12.90	4.00	8.59	10.75	9.39
⑪人　事	58.06	64.00	69.53	56.99	63.54
⑫—1 暗号鍵	48.39	20.00	33.59	38.71	35.74
⑫—2 ⑫その他	0.00	0.00	5.47	4.30	3.97
⑬その他	0.00	0.00	0.78	13.98	5.05
各層のケース数	100.00	100.00	100.00	100.00	100.00
度　数	31	25	128	93	277

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞ ）

（表－31）

〔横の問〕　1.2　年間売上高

〔縦の問〕　4.　不正入手，不正漏示の潜在的脅威を強く意識している重要な情報としては，どのようなものがありますか。

（単位：％）　　（金融機関以外）

項　目	① 10以下	② 10～	③ 100	④ 1000	⑤ 5000	⑥ 1兆	合　計
①　開発技術	33.33	20.00	20.87	17.65	100.00	57.14	22.79
②－1受発注	25.00	11.11	35.65	41.18	100.00	42.86	31.63
②－2販　売	25.00	26.67	46.96	55.88	100.00	57.14	43.72
②－3仕入れ	25.00	15.56	33.91	35.29	100.00	42.86	30.70
②－4外注管理	25.00	4.44	11.30	14.71	100.00	42.86	13.02
②－5在庫管理	16.67	15.56	33.04	38.24	100.00	57.14	30.70
③－1信用情報	33.33	22.22	26.96	26.47	100.00	42.86	27.44
③－2リスト	33.33	42.22	45.22	55.88	100.00	71.43	46.98
③－3暗証番号	0.00	8.89	5.22	11.76	50.00	28.57	7.91
③－4③その他	0.00	0.00	0.87	2.94	0.00	0.00	0.93
④　需要予測	8.33	0.00	11.30	20.59	100.00	42.86	12.09
⑤　事業計画	8.33	6.67	7.83	17.65	50.00	42.86	10.70
⑥－1収　支	25.00	33.33	40.87	38.24	50.00	85.71	39.53
⑥－2資産負債	25.00	35.56	40.00	41.18	50.00	100.00	40.47
⑥－3原価計算	33.33	37.78	46.96	32.35	100.00	85.71	43.72
⑥－4⑥その他	0.00	4.44	2.61	5.88	0.00	28.57	4.19
⑦－1資金移動	16.67	17.78	14.78	26.47	50.00	42.86	18.60
⑦－2貸　借	8.33	11.11	16.52	29.41	50.00	57.14	18.60
⑦－3投　資	8.33	13.33	12.17	17.65	50.00	57.14	14.88
⑦－4⑦その他	0.00	0.00	0.87	2.94	0.00	0.00	0.93
⑧　設　備	8.33	0.00	6.09	11.76	50.00	42.86	7.44
⑨　不動産	0.00	2.22	4.35	14.71	50.00	42.86	6.98
⑩　株　主	8.33	11.11	7.83	11.76	50.00	28.57	10.23
⑪　人　事	50.00	60.00	65.22	85.29	100.00	100.00	67.91
⑫－1暗号鍵	16.67	42.22	28.70	38.24	50.00	57.14	33.49
⑫－2⑫その他	0.00	4.44	6.09	2.94	0.00	0.00	4.65
⑬　その他	8.33	8.89	1.74	0.00	0.00	0.00	3.26
各層のケース数	100.00	100.00	100.00	100.00	100.00	100.00	100.00
度　数	12	47	120	40	2	7	228

〔層別集計表（各層別ケース数に対する割合<層：横の問>）

（表－32）

〔横の問〕　1.2　預金残高

〔縦の問〕　4.　不正入手，不正漏示の潜在的脅威を強く意識している重要な情報としては，どのようなものがありますか。

（単位：%）　　（金融機関）

項　目	① 5千以下	② ～5000	③ 1兆	④ 5兆	⑤ 10兆	合　計
①　開発技術	0.00	0.00	0.00	0.00	0.00	0.00
②－1 受発注	0.00	0.00	33.33	0.00	0.00	5.26
②－2 販　売	40.00	50.00	100.00	0.00	0.00	47.37
②－3 仕入れ	40.00	50.00	100.00	0.00	0.00	47.37
②－4 外注管理	0.00	0.00	0.00	0.00	0.00	0.00
②－5 在庫管理	0.00	0.00	33.33	0.00	0.00	5.26
③－1 信用情報	80.00	75.00	100.00	0.00	100.00	84.21
③－2 リスト	60.00	75.00	100.00	0.00	100.00	73.68
③－3 暗証番号	80.00	100.00	100.00	0.00	100.00	89.47
③－4 ③その他	0.00	0.00	0.00	0.00	0.00	0.00
④　需要予測	0.00	0.00	0.00	0.00	0.00	0.00
⑤　事業計画	0.00	0.00	0.00	0.00	0.00	0.00
⑥－1 収　支	10.00	0.00	33.33	0.00	50.00	15.79
⑥－2 資産負債	10.00	0.00	66.67	0.00	50.00	21.05
⑥－3 原価計算	0.00	0.00	0.00	0.00	50.00	5.26
⑥－4 ⑥その他	0.00	0.00	0.00	0.00	0.00	0.00
⑦－1 資金移動	20.00	0.00	33.33	0.00	100.00	26.32
⑦－2 貸　借	30.00	0.00	33.33	0.00	50.00	26.32
⑦－3 投　資	0.00	0.00	33.33	0.00	50.00	10.53
⑦－4 ⑦その他	0.00	0.00	0.00	0.00	0.00	0.00
⑧　設　備	0.00	0.00	33.33	0.00	0.00	5.26
⑨　不動産	0.00	0.00	33.33	0.00	0.00	5.26
⑩　株　主	20.00	0.00	0.00	0.00	50.00	15.79
⑪　人　事	60.00	75.00	100.00	0.00	100.00	73.68
⑫－1 暗号鍵	30.00	100.00	66.67	0.00	100.00	57.89
⑫－2 ⑫その他	0.00	0.00	0.00	0.00	0.00	0.00
⑬　そ の 他	0.00	0.00	0.00	0.00	0.00	0.00
各層のケース数	100.00	100.00	100.00	0.00	100.00	100.00
度　数	10	4	3	0	2	19

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－33）

〔横の問〕　1.3　従業員数（常勤）

〔縦の問〕　4.　不正入手，不正漏示の潜在的脅威を強く意識している重要な情報としては，どのようなものがありますか。

（単位：％）

項　　目	① 3百以下	② 300～	③ 1000	④ 5000	⑤ 1万	合　計
①　開発技術	14.06	14.74	21.35	26.67	50.00	18.68
②－1 受発注	12.50	25.26	33.71	40.00	40.00	26.37
②－2 販　　売	25.00	41.05	50.56	40.00	40.00	40.29
②－3 仕入れ	17.19	26.32	39.33	40.00	40.00	29.67
②－4 外注管理	3.13	7.37	15.73	20.00	40.00	10.99
②－5 在庫管理	17.19	22.11	32.58	26.67	40.00	25.27
③－1 信用情報	35.94	21.05	34.83	46.67	70.00	32.23
③－2 リスト	39.05	40.00	51.69	53.33	80.00	45.79
③－3 暗証番号	15.63	11.58	16.85	20.00	50.00	16.12
③－4 ③その他	1.56	1.05	0.00	6.67	0.00	1.10
④　需要予測	1.56	9.47	13.48	13.33	40.00	10.26
⑤　事業計画	3.13	3.16	16.85	13.33	30.00	9.16
⑥－1 収　　支	26.56	32.63	37.08	46.67	60.00	34.43
⑥－2 資産負債	21.88	34.74	38.20	53.33	70.00	35.16
⑥－3 原価計算	21.88	35.79	43.82	40.00	70.00	36.63
⑥－4 ⑥その他	3.13	2.11	5.62	6.67	10.00	4.03
⑦－1 資金移動	9.38	13.68	20.22	40.00	60.00	17.95
⑦－2 貸　　借	9.38	15.79	20.22	33.33	50.00	17.95
⑦－3 投　　資	6.25	11.58	15.73	26.67	30.00	13.19
⑦－4 ⑦その他	0.00	1.05	1.12	0.00	0.00	0.73
⑧　設　　備	3.13	2.11	10.11	13.33	20.00	6.23
⑨　不動産	1.56	4.21	7.87	13.33	30.00	6.23
⑩　株　　主	7.81	11.58	5.62	13.33	30.00	9.52
⑪　人　　事	45.31	62.11	73.03	86.67	90.00	64.10
⑫－1 暗号鍵	29.69	28.42	42.70	60.00	60.00	36.26
⑫－2 ⑫その他	1.56	5.26	4.49	6.67	0.00	4.03
⑬　その他	9.38	3.16	5.62	0.00	0.00	5.13
各層のケース数	100.00	100.00	100.00	100.00	100.00	100.00
度　　数	64	95	89	15	10	273

〔層別集計表（各層別ケース数に対する割合＜層：横の間＞）

（表－34）

〔横の問〕　1.5　コンピュータ・システムへの投資規模（レンタルの場合は売価換算）

〔縦の問〕　4.　不正入手，不正漏示の潜在的脅威を強く意識している重要な情報とは，どのようなものがありますか。

（単位：％）

項　目	①5千以下	②～5000	③1億	④10億	⑤30億	⑥50億	⑦100億	合　計
①　開発技術	15.79	5.71	20.83	26.32	13.33	0.00	30.00	18.66
②—1受発注	15.79	14.29	29.17	31.58	13.33	28.57	30.00	25.75
②—2販　売	26.32	37.14	40.97	52.63	13.33	57.14	30.00	39.55
②—3仕入れ	31.58	11.43	31.94	34.21	13.33	42.86	30.00	28.73
②—4外注管理	5.26	2.86	11.81	13.16	0.00	14.29	20.00	10.07
②—5在庫管理	21.05	22.86	25.69	34.21	0.00	14.29	20.00	24.25
③—1信用情報	10.53	14.29	28.47	47.37	46.67	85.71	40.00	30.97
③—2リスト	21.05	31.43	43.75	60.53	53.33	85.71	50.00	44.78
③—3暗証番号	0.00	5.71	11.11	34.21	33.33	57.14	20.00	15.67
③—4③その他	0.00	0.00	1.39	0.00	0.00	0.00	10.00	1.12
④　需要予測	0.00	2.86	9.72	21.05	0.00	0.00	20.00	9.33
⑤　事業計画	0.00	0.00	11.11	15.79	0.00	0.00	20.00	8.96
⑥—1収　支	36.84	28.57	31.94	47.37	6.67	57.14	50.00	33.96
⑥—2資産負債	42.11	25.71	32.64	47.37	13.33	57.14	50.00	34.70
⑥—3原価計算	47.37	31.43	38.19	36.84	20.00	14.29	40.00	36.19
⑥—4⑥その他	10.53	2.86	3.47	5.26	0.00	0.00	20.00	4.48
⑦—1資金移動	26.32	5.71	15.97	23.68	13.33	28.57	40.00	17.54
⑦—2貸　借	21.05	5.71	16.67	28.95	6.67	28.57	30.00	17.54
⑦—3投　資	26.32	2.86	11.11	18.42	0.00	42.86	20.00	12.69
⑦—4⑦その他	0.00	0.00	1.39	0.00	0.00	0.00	0.00	0.75
⑧　設　備	0.00	0.00	6.25	15.79	0.00	14.29	10.00	6.34
⑨　不動産	0.00	0.00	4.86	15.79	0.00	14.29	20.00	5.97
⑩　株　主	10.53	5.71	9.03	18.42	0.00	0.00	10.00	9.33
⑪　人　事	57.89	62.85	57.64	84.21	66.67	85.71	70.00	63.81
⑫—1暗号鍵	15.79	20.00	36.11	50.00	53.33	57.14	40.00	36.19
⑫—2⑫その他	0.00	0.00	4.86	5.26	6.67	0.00	0.00	3.73
⑬　その他	5.26	2.86	8.33	0.00	0.00	0.00	0.00	5.22
各層のケース数	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00
度　数	19	35	144	38	15	7	10	268

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－35）

〔横の問〕　1.5　コンピュータシステムへの投資規模（レンタルの場合は売価換算）

〔縦の問〕　.5.2　セキュリティ対策の腹路としては，どのようなものが重視されますか。（複数回答）

（単位：％）

項　　目	①5千以下	②5000	③1億	④10億	⑤30億	⑥50億	⑦100億	合　計
①費　　用	63.16	59.38	70.08	80.56	78.57	57.14	70.00	69.80
②－1アクセス	26.32	43.75	49.61	36.11	64.29	57.14	50.00	46.12
②－2暗号化	5.26	21.88	21.26	25.00	21.43	57.14	40.00	22.45
②－3相　互	21.05	15.63	20.47	16.67	0.00	14.29	0.00	17.14
②－4受渡し	26.32	12.50	12.60	11.11	7.14	0.00	0.00	12.24
②－5入退室	26.32	28.13	17.32	11.11	14.29	0.00	10.00	17.55
②－6規その他	0.00	0.00	0.00	0.00	0.00	14.29	0.00	0.41
③管　　理	10.53	21.88	14.17	8.33	0.00	0.00	0.00	12.24
④内　　部	47.37	46.88	56.69	63.89	78.57	57.14	60.00	57.14
⑤そ の 他	0.00	6.25	0.00	0.00	7.14	0.00	10.00	1.63
各層のケース数	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00
度　　数	19	32	127	36	14	7	10	245

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－36）

〔横の問〕　1.2　年間売上高

〔縦の問〕　6.1　貴社では，就業規則や従業員との間の契約で，企業秘密の保持に関し定めていますか。（複数回答）

（単位：％）　　（金融機関以外）

項　目	①10以下	②10～	③100	④1000	⑤5000	⑥1兆	合　計
①　就業規定	81.82	72.34	85.59	79.49	100.00	100.00	82.14
②　契　約	36.36	12.77	3.39	17.95	50.00	14.29	10.27
③　な　い	0.00	23.40	12.71	12.82	0.00	0.00	13.84
各層のケース数	100.00	100.00	100.00	100.00	100.00	100.00	100.00
度　数	11	47	118	39	2	7	224

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－37）

〔横の問〕　1.2　預金残高

〔縦の問〕　6.1　貴社では，就業規則や従業員との間の契約で，企業秘密の保持に関し定めていますか。

（単位：％）　　（金融機関）

項　目	①5千以下	②5000～	③1兆	④5兆	⑤10兆	合　計
①　就業規定	80.00	100.00	100.00	0.00	100.00	90.48
②　契　約	10.00	16.67	0.00	0.00	0.00	9.52
③　な　い	20.00	0.00	0.00	0.00	0.00	9.52
各層のケース数	100.00	100.00	100.00	0.00	100.00	100.00
度　数	10	6	3	0	2	21

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－38）

〔横の問〕　1.2　年間売上高

〔縦の問〕　6.2　どのような内容の定めをしていますか。（複数回答）

（単位：％）　　（金融機関以外）

項　目	①10以下	②10～	③100	④100	⑤5000	⑥1兆	合　計
①在職中	72.73	69.44	77.45	66.67	50.00	85.71	73.82
②退職後	54.55	33.33	25.49	30.30	50.00	0.00	28.80
③携わる	0.00	0.00	0.00	6.06	0.00	0.00	1.05
④期　間	0.00	0.00	0.98	6.06	0.00	0.00	1.57
⑤抽象的	9.09	33.33	38.24	57.58	100.00	28.57	39.27
⑥具体的	0.00	5.56	0.98	3.03	0.00	0.00	2.09
⑦その他	0.00	2.78	0.00	6.06	0.00	28.57	2.62
各層のケース数	100.00	100.00	100.00	100.00	100.00	100.00	100.00
回答数	11	36	102	33	2	7	191

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－39）

〔横の問〕　1.2　預金残高

〔縦の問〕　6.2　どのような内容の定めをしていますか。

（単位：％）　　（金融機関）

項　目	①5千以下	②5000～	③1兆	④5兆	⑤10兆	合　計
①在職中	25.00	83.33	100.00	0.00	0.00	52.63
②退職後	62.50	33.33	0.00	0.00	100.00	47.37
③携わる	0.00	0.00	0.00	0.00	0.00	0.00
④期　間	12.50	0.00	0.00	0.00	0.00	5.26
⑤抽象的	50.00	66.67	66.67	0.00	50.00	57.89
⑥具体的	0.00	0.00	0.00	0.00	0.00	0.00
⑦その他	0.00	0.00	0.00	0.00	0.00	0.00
各層のケース数	100.00	100.00	100.00	0.00	100.00	100.00
度　数	8	6	3	0	2	19

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－40）

〔横の問〕　1.2　年間売上高

〔縦の問〕　7.　受情報の不正入手，不正漏示を刑事上の犯罪とし処罰する立法について，どのように考えますか。

（単位：％）　　（金融機関以外）

項　目	①10以下	②10～	③100	④1000	⑤5000	⑥1兆	合　計
①必　要	18.18	23.26	37.17	27.03	50.00	16.67	31.13
②明確化	18.18	39.53	25.66	27.03	50.00	33.33	28.77
③不必要	63.64	39.53	37.17	51.35	0.00	50.00	41.51
④その他	0.00	0.00	1.77	0.00	0.00	0.00	0.94
各層のケース数	100.00	100.00	100.00	100.00	100.00	100.00	100.00
度　数	11	43	113	37	2	6	212

〔層別集計表（各層別ケース数に対する割合＜層：横の問＞）

（表－41）

〔横の問〕　1.3　従業員数（常勤）

〔縦の問〕　7.　受情報の不正入手，不正漏示を刑事上の犯罪とし処罰する立法について，どのように考えますか。

（単位：％）

項　目	①3百以下	②300～	③1000	④5000	⑤1万	合　計
①必　要	29.85	35.11	30.59	47.06	44.44	33.46
②明確化	32.84	30.85	27.06	47.06	33.33	31.25
③不必要	37.31	35.11	44.71	17.65	33.33	37.50
④その他	0.00	2.13	1.18	0.00	0.00	1.10
各層のケース数	100.00	100.00	100.00	100.00	100.00	100.00
度　数	67	94	85	17	9	272

付　録　日本におけるコンピュータ犯罪の事例

(1) コンピュータの不正操作 …… 107
(2) データ，プログラムの不正入手 …… 113
(3) コンピュータの無権限使用 …… 115
(4) プログラムの改ざん，消去 …… 116
(5) コンピュータの破壊 …… 117
(6) ＣＤ犯罪 …… 118
a．キャッシュ・カードの偽造 …… 118
b．キャッシュ・カードの窃用 …… 119
c．オンライン悪用事件 …… 121
(7) その他のコンピュータ関連犯罪 …… 122
a．通帳等偽造事件 …… 122
b．入力帳票等の悪用 …… 122
c．シンボル …… 123
(8) コンピュータに関与が不明 …… 124

1. コンピュータの不正操作

(1) 岡村製作所事件（昭和48年1月告訴）

① 業務上横領（刑法第253条）

② 東京地検へ送検（昭和48年4月）

③ 元販売事務係長が，製品の売掛金を会社名義の口座には振込まず，予め用意した架空口座に振込んだ上で会社のコンピュータには振込みがあったように打ち込み，取引先には正規の領収書を渡し，さらに会社の収入伝票を破棄して証拠を隠すなどして計約4000万円を横領した。

(2) 中国銀行事件（昭和50年6月検挙）

① 詐欺（刑法第246条1項）（有印私文書偽造・同行使）

② 懲役3年（別件背任，業務上横領を含む） 岡山地裁判昭52.3.29

③ 同銀行行員が，本支店間の預金業務がオフラインであり，しかも元帳残高照会が月に1度であることに目をつけ，架空口座の普通預金通帳及び普通預金払戻請求書等を作成した上で，普通預金会計機を操作して金員を騙取した。被害金額は集金横領の分を含めて約7500万円。

(3) 東天紅事件（昭和50年5月）

① 業務上横領（刑法第253条）

②

③ 人事係長が給与計算について退職者リストを抹消せず，退職者分の給与を騙取した。被害金額は，約4000万円といわれる。

(4) 北海道拓殖銀行事件（昭和51年10月）

① 業務上横領（刑法第253条）

②

③ 同行女子行員が残金の僅かな自分名義の口座に92万円の架空振込みを行い，CDから内40万円を引き出した。

(5) 山口銀行事件（昭和54年11月検挙）

① 業務上横領（刑法第253条）

② 被告人A 懲役7年（別件背任罪も含む） 山口地裁下関支部判昭56.

12.2 （確定）

被告人B　懲役3年　山口地裁下関支部判昭56.12.2（控訴）

（控訴審）懲役3年　広島高裁判

被告人C　懲役6年　山口地裁下関支部判昭60.1.30（控訴）

(6) 滑川市農協事件（昭和54年9月）

① 詐欺（刑法第246条1項）

② 懲役2年6か月（執行猶予3年）　富山地裁判昭55.6.24

(7) 西京コクヨ事件（昭和54年11月）

① 業務上横領（刑法第253条）

②

③ 女子社員が入力伝票を偽造した上で，自らコンピュータを操作し1000万円余りを横領した。

(8) 三和銀行事件（昭和56年9月検挙）

① 有印私文書偽造（刑法第159条1項）・同行使（第161条1項）詐欺（第246条1項）

② 被告人A　懲役5年

被告人B　懲役2年6か月　大阪地裁判昭57.7.27（確定）

(9) 中野市農協事件（昭和56年9月検挙）

① 詐欺（刑法第246条1項）

② 懲役2年6か月　長野地裁判昭57.3.18

(10) 北浜クレジット社事件（昭和56年10月検挙）

① 業務上横領（刑法第253条）

② 懲役2年6か月（執行猶予5年）　大阪地裁判昭57.3.2

(11) 平和相互銀行事件（昭和56年10月）

① 詐欺（刑法第246条1項）

② 未解決

(12) 秋田相互銀行事件（昭和56年11月）

① 業務上横領（刑法第253条）

②

(13) 神奈川県庁事件（昭和57年6月検挙）

① 詐欺（刑法第246条1項）

②

③ 県出納事務職員が，移転補償等の名目で，コンピュータによる起票機を使用するなどして支出伝票を偽造し，予め開設しておいた架空人名義の預金口座に振込ませ，前後30回にわたり，県から約1億2000万円を騙取した。事件の発覚が遅れたのは，起票機のフロッピー・ディスクに記録された伝票データに基づく支出集計表による照合作業が，同職員の職務であったことによるものであった。

(14) 羽合町農協事件（昭和57年1月）

① 業務上横領（刑法第253条）

②

③ 同組合の女子職員が顧客の普通預金口座から不正に払い戻し処理を行ったり，共済満期の掛金払戻金を自分名義の預金口座に振替れるなどして560万円を横領した。

(15) 島根農協事件（昭和58年2月検挙）

① 業務上横領（刑法第253条）

②

③ 農協支所長が貸付けを装って架空の伝票を作成し，これを端末装置から入力して，予め開設しておいた架空人名義の普通預金口座に振込むという方法で現金735万円を横領した。

(16) 秋田県警免許証不正交付事件（昭和59年5月検挙）

① 虚偽有印公文書作成（刑法第156条）・枉法収賄（刑法第197条の31項）

② 主犯　懲役3年10か月，追徴金223万円　秋田地裁判昭60.2.27

③ 自動車の運転免許証の審査，登録等に関する職務に従事していた警察官が，無免許者のため免許を取得している旨の虚偽の登録原簿を作成し，係員をして端末装置から警察情報処理センターの電子計算機にその旨送信させ，同計算機の磁気ファイルにその登録をした上，亡失等を理由とする免許証再交付申請をさせ，端末機により免許を取得している旨のデ

ータを出力させて，これを印磁処理した免許台紙を作成させ，機械処理により，係員に合計43通の運転免許証を作成させた。

(17) 愛媛相互銀行事件（昭和59年1月検挙）

① 私文書偽造（刑法第159条）

②

(18) 丹波農協事件（昭和59年12月検挙）

① 背任（刑法第247条）

②

(19) 福岡農協事件（昭和59年2月検挙）

① 業務上横領（刑法第253条）

②

③ 農協支所長ほか3人が，架空の貯金受入伝票を作成し，端末装置を操作して，共犯者名義の当座勘定に架空入金打込みを行い，これを隠蔽するため架空名義人らに対する偽造貸付伝票を作成するなどの方法により，顧客から預り保管中の金員の中から前後7回にわたり合計4億1041万円を横領した。

(20) 矢野町農協事件（昭和59年3月検挙）

① 背任（刑法第247条）

②

(21) 広島みどりの窓口事件（昭和56年8月検挙）

① 有価証券偽造（刑法第162条）・同行使（第163条）
詐欺（刑法第246条1項）

②

(22) 大阪サラ金事件（昭和59年9月検挙）

① 業務上横領（刑法第253条）

②

③ サラ金会社の支店長が，同店の顧客名義を利用して，端末機から借入金の架空返済及び架空貸付処理をするなどの方法により，同店営業資金の中から前後34回にわたり約500万円を横領した。

(23) 大阪殖産信用金庫事件（昭和59年4月検挙）

① 詐欺（刑法第246条1項）

②

(24) 国鉄事件（昭和59年11月検挙）

① 詐欺（刑法第246条1項）

②

③ 元国鉄職員ほか1人が，自己及び職員の昇格・昇給に関するデータを偽造するとともに，情を知らない職員に端末装置を操作させ同データを入力し，不正に昇格・昇給させた。

(25) 秋田農協事件（昭和59年9月）

① 背任（刑法第247条）

② 立件なし

③ 秋田県の農協の端末機の操作権限を有する貸付係職員が，農協オンラインの端末装置を不正に操作して，実父が同農協から借り受けた150万円中100万円を返済したように処理した。

(26) 福岡銀行通帳偽造事件（昭和61年3月検挙）

① 有印私文書偽造（刑法第159条1項）・同行使（第161条1項）
盗（刑法第235条）

② 公判請求　昭61.4.8

③ 福岡銀行にプログラマとしてシステム開発のため派遣されていたコンピュータソフトウェア開発会社の技術社員が，端末機を操作して，同銀行のコンピュータに入力されたデータから他人の口座番号，預金残高，暗証番号等のデータを検索抽出し，長女名義の通帳の磁気テープに上記口座番号を印磁した上，現金自動支払機に差し込んで暗証番号を打ち込み，現金を引き出した。［資料1－26］

(27) 東京信用組合事件（昭和60年1月検挙）

① 業務上横領（刑法第253条）

②

㉘ 兵庫県市役所事件（昭和60年9月検挙）

① 詐欺（刑法第246条第1項）

②

③ 兵庫県下の市役所の福祉課主事が，架空の児童手当受給者を作出し，架空預金口座を開設した上，虚偽の電算入力表を作成し，情を知らない係員に振込入金させ，前後121回にわたり合計1356万4000円を騙取した。

㉙ 田宮町農協事件（昭和61年6月）

① 業務上横領（刑法253条）

②

2. データ・プログラムの不正入手

(1) リーダーズ・ダイジェスト事件（昭和46年2月）

① 物故買（刑法第256条2項）

② 告訴の後，和解成立し不起訴。

(2) 日本チャリティ・プレート事件（昭和53年6月）

①

② 示談が成立。

(3) プロミス事件（昭和56年11月）

① 詐欺（刑法第246条1項）

②

(4) 北海道銀行キャッシュカード偽造事件（昭和57年2月検挙）

ＣＤ犯罪の6(5)参照

(5) 新潟鉄工事件（昭和58年2月検挙）

① 業務上横領（刑法第253条）・詐欺未遂（刑法第253条第1項・第250条）

② 被告人Ａ　懲役2年6か月（執行猶予3年）
被告人Ｂ　懲役1年6か月（執行猶予3年）
被告人Ｃ　懲役1年　（執行猶予2年）東京地裁判60.2.13（一部控訴）

③ コンピュータの利用による自動設計製図システム開発を担当していた新潟鉄工部長代理ほか5名は，共謀の上，業務上保管していた同システムに関する各種設計書等の資料をコピーのため社外に持ち出した。

(6) 総合コンピュータ事件（昭和59年6月検挙）

① 背任（刑法第247条）

② 被告人ＡＢ　懲役1年6か月（執行猶予3年）　東京地裁判昭60.3.6（確定）

(7) 医師会事件（昭和59年7月検挙）

① 窃盗（刑法第235条）

②

③ 愛知県下の社団法人医師会臨床検査センターの元集団検診部長は，同センター所長が管理する「臨床検査業務処理システムプログラム」の複製磁気テープ1巻（時価3000万円相当）を窃取した。

(8) 軽自動車協会連合会事件（昭和61年4月検挙）

① 盗（刑法第235条）

② 被告人ＡＢＣ 懲役2年（執行猶予4年） 東京地裁判昭61.9.8

③ 全国軽自動車協会連合会業務課長が，全国の軽自動車1200万台に関する車両番号，形式，使用者の指名，住所等を記録した磁気テープ24巻を窃取し，共犯者がこれをコピーし，同日これを返還し，同コピーを売却したもの。

(9) ＫＤＤビーナスＰ侵入事件（昭和60年5月）

①

② 未解決

③ a．米国系電気製造会社は，ＫＤＤのビーナスＰを利用して米国の本社との間に在庫管理等の情報交換を行っていたところ，パスワードが盗用され，ビーナスＰの回線が無断使用されて，米国の10数会社のデータベース（上記会社との間に利用契約なし）からホビー情報等各種の情報が引き出された。

b．東京の機械器具会社はＫＤＤとビーナスＰ契約を結び，会社内の大型コンピュータと海外支店の端末機をビーナスＰで結んでいたが，西ドイツから数回にわたって大型コンピュータに侵入され，ソフトウェアの人事管理ファイル等に無関係な言葉等が記録された（“落書きされた”）ほか，東京のデータベース会社のコンピュータには英・仏から，また，大学研究所の大型コンピュータにも西ドイツ・スイスから侵入を受けた。

3. コンピュータの無権限使用

(1) 日本鉄道建設公団事件（昭和56年9月）

① 賭博（刑法第185条）

② 東京地検　不起訴

③ 日本鉄道建設公団工事第6課係長ほか106名が，第63回全国高校野球選手権大会がめぐり大規模な「野球トトカルチョ」を行い，賭博計算と配当金計算に業務用のコンピュータを不正に使用した。

(2) 岡山大学計算センター事件（昭和56年10月）

①

② 立件なし

(3) ＫＤＤビーナスＰ侵入事件（昭和60年5月）

データ・プログラムの不正入手2(9)参照

(4) 「トリスタン」事件（昭和62年2月）

①

② 行為者不明

③ 文部省の高エネルギー物理学研究所（筑波研究学園都市）における大型加速器「トリスタン」計画の国際協同研究用コンピュータが，西ドイツのハッカーグループに国際データ通信回線を通じて侵入を受けた上，事務用のファイルの一部が壊されたり，落書きされたりした。

4. プログラムの改竄・消去

(1) 大阪工業大学事件（昭和59年3月）

①

② 告訴なし

③ 大阪工業大学中央研究所のコンピュータの磁気ディスクに納められた教授等の学術用プログラム等約1500件のデータが消去された。

5. コンピュータの破壊

(1) コクヨ事件（昭和48年3月）

① 器物損壊（刑法第261条）

②

③ 元社員が飲酒酩酊のうえコンピュータ室に侵入し，手当り次第に暴れて機器類に被害を与えた。

(2) 間組本社ビル爆破事件（昭和50年2月）

① 爆発物取締罰則違反（同罰則1条）・殺人未遂（刑法第199条・203条）

② 死刑（別件爆発物取締罰則違反，殺人，殺人未遂，殺人予備を含む）
東京地裁判昭54.11.12（控訴） 東京高裁判昭57.10.29（上告）

③ 東アジア反日武装戦線のメンバー6名が，港区の間組本社6階の営業本部，9階の開発部パンチテレックス室に爆発物を仕掛けて爆発・全焼させ，約20億円の被害を与えた。

(3) 航空管制データ通信ケーブル切断事件（昭和53年5月）

① （航空法）

② 未検挙

(4) 山口パチンコ店事件

① 威力業務妨害（刑法第224条）

②

③ 暴力団組員ら数人が，山口県下のパチンコ店の経営者がディナーショー入場券の買取方を拒否したことに対して仕返しを企図し，同店に赴き，つるはしや角材を用いて同店内に設置された制御用コンピュータを破壊し，営業不能に陥れた。

6. ＣＤ犯罪

ａ．キャッシュカードの偽造

(1) 伏見信用金庫事件（昭和49年12月検挙）

① 有印私文書偽造（刑法第159条第1項）・同行使（第161条第1項）
窃盗（第235条第1項） －＞ 電磁的記録の不正作出（刑法第161条の2）

②

(2) 近畿相互銀行事件（昭和56年10月）

① 有印私文書偽造（刑法第159条第1項）・同行使（第161条第1項）
窃盗（刑法第235条） －＞ 電磁的記録の不正作出（刑法第161条の2）

② 懲役4年6か月（別件公正証書原本不実記載，同行使，出入国管理令違反，外国為替及び外国貿易管理法違反を含む） 大阪地裁判昭57.9.9（確定）

(3) 宮城第一信用金庫事件（昭和56年3月）

① 有印私文書偽造（刑法第159条第1項）・同行使（第161条第1項）
窃盗（刑法第235条） －＞ 電磁的記録の不正作出（刑法第161条の2）

② 未解決

③ 同信用金庫本店現金自動支払コーナーのＣＤにおいて，クレジットカードの表上部に現金の払戻しに必要なコードを記録した磁気テープを貼り付け偽造したキャッシュカードによって現金49万9000円が引き出された。

(4) 八戸信用金庫事件（昭和56年5月）

① 有印私文書偽造（刑法第159条第1項）・同行使（第161条第1項）
窃盗（刑法第235条） －＞ 電磁的記録の不正作出（刑法第161条の2）

② 未解決

(5) 北海道銀行キャッシュカード偽造事件（昭和57年2月検挙）

① 公衆電気通信法違反（同法第112条第1項）・窃盗（刑法第235条）

② 懲役2年6か月（執行猶予4年） 札幌地裁判昭59.3.27（確定）

③ 電電公社職員が，通信回線から銀行のオンライン取引データを盗聴し，これを自己のキャッシュカードに記録されている情報をもとに解読した上でキャッシュカードを偽造し，これを使って3箇所のCDから133万円を盗み出した。

b．キャッシュカードの窃用

(6) 三菱銀行府中支店事件（昭和49年12月）

① 窃盗（刑法第235条）

②

(7) 三井銀行堀留支店事件（昭和50年2月）

① 窃盗（刑法第235条）・業務上横領（第253条）

②

(8) 第一勧業銀行福山支店事件（昭和50年4月）

① 窃盗（刑法第235条）

②

(9) 山形銀行新庄支店事件（昭和53年3月）

① 窃盗（刑法第235条）

②

(10) 北海道銀行北栄支店事件（昭和56年10月）

① 窃盗（刑法第235条）・詐欺（刑法第246条第1項）

②

(11) 北海道キャッシュカード窃用事件（昭和57年1月検挙）

① 窃盗（刑法第235条）

②

③ 大学生が同じ下宿の大学生のキャッシュカードを盗み出し，CDから15

万円を引き出した。暗証番号は，以前被害者が風邪で寝込み，現金の引き出しを依頼した際に教えられていた。

(12) 長野キャッシュカード窃用事件（昭和57年6月検挙）

① 窃盗（刑法第235条）

②

③ 保険外交員が，駐車中の乗用車からキャッシュカード，運転免許証等を盗み取り，運転免許証から被害者の本籍，住所の番地，生年月日，電話番号等を調べ，これらの中から生年月日の数字を試し打ちしたところ，これが暗証番号と合致し，38万4000円を引き出した。

(13) 大阪キャッシュカード窃用事件（昭和58年3月検挙）

① 窃盗（刑法第235条）

②

③ 無職者が，テニスクラブの更衣室等から約10か月の間に窃取した32人分のキャッシュカードを使用して，現金約1147万円を引き出した。暗証番号を知った方法は，運転免許証等から生年月日を知って推測したもの17件，銀行員等を装って被害者から聞き出したもの14件，キャッシュカードとともに暗証番号のメモ書きを入手したもの1件であった。

(14) 埼玉キャッシュカード窃用事件（昭和59年6月検挙）

① 窃盗（刑法第235条）

②

③ 印刷業経営者が，一般住宅に空巣に入って窃盗したキャッシュカードを使用して，現金約1348万円を引き出した。暗証番号は，一緒に盗み出した健康保険証に記載された生年月日等から推測していた。

(15) 鹿児島キャッシュカード窃用事件（昭和60年9月検挙）

① 窃盗（刑法第235条）

②

③ 主婦が，窃取したキャッシュカードを使用して，CDから現金約11万円を引き出した。暗証番号は，同カード名義人の住民票から推測していた。

(16) 愛媛キャッシュカード窃用事件（昭和60年9月検挙）

① 窃盗（刑法第235条）

②

③ サラ金会社女子事務員が，勤務先のコンピュータ端末機を使って，拾得したキャッシュカードの暗証番号を解読し，ATMを操作の上，現金47万円を窃取した。

(17) 福井キャッシュカード窃用事件（昭和61年5月検挙）

① 窃盗（刑法第235条）

②

③ 無職の男が特急列車内において乗客の背広内ポケットから現金やキャッシュカードをすり取り，翌日早朝，被害者宅に警察官を装って電話し，暗証番号を聞出した上でCDから現金114万円を引き出した。

c．オンライン悪用事件

(18) 真由子ちゃん誘拐事件（昭和49年8月検挙）

① 身代金拐取（刑法第225条の2第1項）・拐取者身代金要求
住居侵入（刑法第130条）

② 懲役10年（別件窃盗，有印公文書偽造，同行使を含む）

千葉地裁松戸支部判昭和50. 4.11

(19) 札幌オンライン誘拐事件（昭和54年2月検挙）

① 身代金拐取（刑法第225条の2第1項）・拐取者身代金要求（同第2項）

② 懲役5年　札幌地裁判昭和54. 9.17

(20) 郵便貯金オンライン事件（昭和56年6月）

① 詐欺（刑法第246条第1項）

②

(21) 下谷郵便局事件（昭和60年5月）

① 窃盗（刑法第235条）

②

(22) ニセ請求書事件（昭和61年5月検挙）

① 詐欺（刑法第246条第1項）

②

7. その他のコンピュータ関連犯罪

a. 通帳等偽造事件

(1) 三井銀行通帳偽造事件（昭和49年11月起訴）

① 有印私文書偽造（刑法第159条第1項）・同行使（第161条第1項）
詐欺（第246条第1項）

②

(2) 八光信用金庫通帳偽造事件（昭和51年5月）

① 有印私文書偽造（刑法第159条第1項）・同行使（第161条第1項）
詐欺（第246条第1項）

②

(3) 御牧農協事件（昭和53年6月検挙）

① 有印私文書偽造（刑法第159条第1項）・同行使（第161条第1項）
詐欺（第246条第1項）

②

(4) 福岡銀行通帳偽造事件（昭和61年3月検挙）

コンピュータの不正操作1(26)参照

(5) 中央競馬会変造馬券事件（昭和61年4月検挙）

① 有印私文書偽造（刑法第159条第1項）・同行使（第161条第1項）
窃盗（第235条） －＞ 電磁的記録の不正作出（第161条の2第1項）

②

b. 入力伝票等の悪用

(6) K信用金庫事件（昭和50年6月）

① 背任（刑法第247条）

② 懲役8年（別件詐欺，業務上横領，有価証券偽造，同行使を含む）

横浜地裁川崎支部判昭55.12.23

(7) M工業事件（昭和51年3月）

① 詐欺（第246条第1項）

② 懲役2年6か月　東京地裁判昭51.11.15

(8) 株式会社ＴＭ事件（昭和53年7月）

① 詐欺（第246条第1項）

② 懲役4年　神戸地裁判昭56.9.19

(9) 新日鉄名古屋製鉄所事件（昭和53年5月検挙）

① 有印私文書偽造（刑法第159条第1項）・同行使（第161条1項）
詐欺（第246条第1項）

②

(10) 大丸神戸支店事件（昭和53年9月検挙）

① 詐欺（第246条第1項）

② 懲役4年　神戸地裁判昭56.9.29

(11) 親和銀行住吉支店事件（昭和53年10月検挙）

① 有印私文書偽造（刑法第159条第1項）・同行使（第161条第1項）
詐欺（第246条第1項）

②

ｃ．シンボル

(12) 佐藤工業事件（昭和57年4月送検）

① 詐欺（第246条第1項）

② 東京地検へ送検

(13) 墨田区立保育園事件（昭和52年12月）

① 詐欺（第246条第1項）

②

③ 区役所員と名乗る男が，コンピュータが故障して計算違いが生じたのでやり直すといって23人分のボーナスを持ち去った。

8. コンピュータの関与が不明

(1) 富士銀行四谷支店事件（昭和56年11月）

① 窃盗（刑法第235条）

② 未解決

昭和63年3月発行

発行所　財団法人 日本情報処理開発協会
東京都港区芝公園3丁目5番8号
機械振興会館内
TEL　(432)－9382

印刷所　山陽株式会社
TEL　(591)　0248(代表)