資料

コンピュータ情報の不正取得・漏示に関する法制的対応
—検討経過の中間報告—

（情報セキュリティと法制度調査研究委員会レポート）

平成元年3月

JIPDEC

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６３年度に実施した「情報化と社会制度等に関する調査研究」の一環としてとりまとめたものです。

「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
〃 川端博	明治大学　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	部長
〃 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
〃 堀部政男	一橋大学　法学部	教授
〃 前田雅英	東京都立大学　法学部	助教授
〃 三木茂	三木法律事務所	弁護士
〃 三輪俱侑	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
〃 小林登	㈶日本情報処理開発協会	常務理事
ゲスト 大野幸夫	日本情報サービス㈱　法務室	室長
〃 椙山敬士		弁護士
〃 吉田正夫		弁護士

目　　次

第１章　問題と背景

1.　コンピュータ情報の不正取得・漏示の類型

「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。」

「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。」　〔62年度当委員会レポート「コンピュータ犯罪と法制度－情報の不正入手について－」（以下「62年度レポート」と略称）P 1, 2, 曽根委員）

コンピュータ情報の不正取得・漏示は、いくつかの観点から分類することができる。①行為の主体、②行為の客体、③行為の態様、④行為の目的、結果の観点から分類すると次のようになる。　（以下６２年９月の委員会提出資料…一部修正）

１－１　行為の主体

(1)　内部と外部

内　部
- 役　員
- 従業員
- 退職した役員
- 退職した従業員

準内部
- 外部から派遣された者
  （派遣技師等）
- 委託先
  （委託事務に従事する者）

外　部
- 第三者
- 提携先
  （提携事務に従事する者）

(2) 複数犯

- 内部の複数
- 外部の複数
- 内部・外部の結託

(3) 専門の技術的知識

- 有る場合
- ない場合

複数犯の場合　専門家を

- 含む場合
- 含まない場合

(4) 守秘義務

- 法律に規定されている場合
- 契約に規定されている場合
  - 契約期間中のみの場合
  - 契約期間終了後に及ぶ場合
- 就業規則に規定されている場合
  - 就労期間中のみの場合
  - 退職後に及ぶ場合
- 規定されていない場合

(5) 当該秘密情報の内容に対する認識

- 知っている場合
- 知らない場合

(6) 当該秘密情報に対する職務上の関係

- 財産的価値のある当該情報の保管を委ねられている場合
- 当該情報の管理に直接関係ある事務に従事する場合
- 職務上当該情報を教示されたに過ぎない場合
- 自己の職務と直接関係がない場合

1－2 行為の客体

(1) 情報の性質

- データ
- プログラム

- 電磁的に貯蔵されている情報
- 電磁的に伝送されている情報

(2) 法的な保護の対象

- 著作権の保護の対象となる情報
- 特許権の保護の対象となる情報
- その他無体財産権の保護の対象となる情報
- 上記以外の情報

- 民法上の財産権の客体
- 上記以外

(3) 情報の保有者

- 企業の情報
- 個人の情報

(4) 情報の内容

- 営業情報
- 個人情報

- 生産方法に関する情報
- 技術情報
- 営業活動に関する情報

(5) 秘密情報と公開情報

- 秘匿された情報
- 製品に組み込まれた情報
  （技術的にアクセスが困難な場合）
- 有償で利用可能な情報

- 専門的な秘密情報
- 一般的な職業上の秘密情報

(6) セキュリティ対策

- 権限のないアクセスに対して保護されている情報
- 上記以外の情報

(7) 情報の価値

- 実質的価値のある情報
- アクセス・コントロールが為されているが実質的価値の乏しい情報

- 利用独占により経済的価値のある情報
- 個人のプライバシー、財産保護に影響ある情報
- 公共の利害に影響ある情報

- 開発コストの多少
- 市場価格
- 情報の独自性
- 陳腐化の有無
- 反社会性の有無

1－3 行為態様

(1) 不正取得（不正探知）

- 媒体ごと持ち出す。
- 媒体を一時持ち出し、情報をコピーして媒体を返還する。
- センター内でコンピュータ内の情報をプリントアウトし、または別の媒体にコピーする。
- コンピュータ内の情報を、通信回線を通じて端末機でプリントアウトし、または別の媒体にコピーする。
- ディスプレイに映し出し、撮影またはメモする。
- 通信中の情報を、通信回線から盗聴する。
- 電波を傍受する。

- 部外者による探知
- 情報を知らない部内者による探知
- 情報を知る部内者の漏示を受けて行う探知

(2) 漏　示

- 媒体ごと持ち出す
- 情報をプリントアウトし、または別の媒体にコピーして持ち出す。
- 口頭で伝える。
- 在職中に、知り得た情報を漏らす。
- 在職中に知り得た情報を、退職後に漏らす。

(3) セキュリティ対策の侵害

- セキュリティ対策を侵害して行う探知
- セキュリティ対策を内部から崩す漏示
- その他の探知、漏示

(4) 不当な方法

- 詐欺、脅迫、恐喝、買収等による場合
- 技術的な装置または方法による場合
- その他の場合

1－4　行為の目的、結果

(1) 行為の目的

- 自己または第三者の利益
- 自己または第三者による利用（窃用）
- 加　害
- 競　業

- 報　道
- 学術研究
- 公共的利益（内部告発、公害調査等）
- 遊　び
- 好意的協力（友人、知人の依頼等）

(2) 行為の結果

- 情報の保有者である企業の財産的利益の侵害またはその他の利益の侵害
- 情報主体である個人のプライバシーの侵害
- 公共の利益の侵害

2. コンピュータ情報の不正取得・漏示の事例

コンピュータ情報の不正取得や漏示は、情報犯罪とコンピュータ犯罪という二つの側面を併せ持っている。情報犯罪という側面においては、文書に記録された情報や、従業員等が職務上知識として保有しているノウハウ等に関して、不正取得や漏示が行われた場合との間に共通性がある。

コンピュータ犯罪という側面においても、オフラインの状態にある情報の化体した媒体を一時社外に持ち出して不正にコピーする場合は、文書について同様の行為をする場合と外形上は酷似している。両者の相違は、コンピュータ情報の場合、大量の情報が媒体に凝縮され、検索、複写等が高速度に可能であるという、技術的、機能的な違いである。これに反し、コンピュータ内のオンライン情報を端末から不正に呼出したり、通信中の情報を傍受する場合は、媒体の移動を伴わずに情報を入手することとなるので、情報そのものを純粋に入手するというコンピュータ犯罪の主要な特徴が外形上も露わとなる。

2.1 日本の事例

(1) 文書に記録された情報については、1960年代の高度成長期に、大企業の製造技術に関する秘密情報を、内部犯の漏示を介して、競争相手の会社が不正に入手するという産業スパイ事件の例が刑事事件としていくつか発生している（大日本印刷事件、鐘淵化学事件、東洋レーヨン事件、信越ポリマー事件）。これが1974年に法制審議会で決定された「改正刑法草案」における「企業秘密漏示罪」の動機となっている。

その後は、コンピュータによる情報処理の進展に伴い下火となり、70年代に顧客リスト（建設調査会事件）、80年代に入試問題（早大事件）、製造技術（新薬産業事件）に関する事件が生じている。

(2) コンピュータ情報については、1971年に既に日経マグロウヒル事件が起こっているが、本格的に発生しはじめるのは1980年代に入ってからである。次のように分類される。

(a) プログラム形態での技術情報や営業情報の不正持ち出しが、従業員の独立、転職等に伴って行われた事例（新潟鉄工所事件、綜合コンピュータ事件）。

(b) 従業員、または事務処理委託先における、顧客リストの不正コピーの事例（日経マグロウヒル事件、フジサンケイリビングサービス事件、軽自動車協会連合会事件、京王百貨店事件、総合法令事件）。

コンピュータ処理により、大量の顧客情報の集積・利用が可能となったことが、これらの事件の背景となっている。

(c) キャッシュカードや通帳偽造の手段として、元従業員や派遣技術者がセンター内で預金者の暗証番号等を入手した事例（近畿相銀事件、福岡銀行事件）。

(d) 通信中のオンライン取引データを盗聴した事例（北海道銀行事件）。

(e) システム・ハッカーが侵入し、コンピュータ内の情報を入手した事例（ＫＤＤヴィーナスＰ事件、西独ハッカー事件）、その他ウィルス・プログラムによる暗証番号の入手が企てられた事例（ＰＣ－ＶＡＮ事件）。

(3) 以上のほか1980年代には、製造技術に関するノウハウ等の漏示が、従業員の引き抜きや、従業員による海外出張先での技術指導、新しい装置の製造請負業者による類似品の製作販売に際して行われたという理由で、民事事件として争われている（エム・シー・エル事件、美濃窯業事件、ボンニー事件）。

［情報の不正取得・漏示に関する主要事例］

(1) 文書に記録された情報

① 大日本印刷事件（1964検挙、東京地判昭40.6.26 ）

同社の従業員が工事見積関係稟議決裁一覧表を、社内で会社の用紙にコピーし、競争相手の会社に売却した。（窃盗）

② 鐘淵化学事件（1965検挙、大阪地判昭42.5.31 ）

同社の元従業員が、在職中配付を受けた塩化ビニール製造技術に関する資料ファイル等を退社後売却した。（業務上横領）

③ 東洋レーヨン事件（1967検挙、神戸地判昭56.3.27 ）

同社の従業員がポリエステル、テトロンフィルム製造装置に関する資料を写真撮影し競争相手の会社に売却した。（背任不成立）

④ 信越ポリマー事件（1969検挙）

外国人留学生が同社のプラスチック成型方法に関する資料を窃取しソビエト大使館員に譲り渡した疑いで検挙された。（不起訴）

⑤ 建設調査会事件（1978、東京地判昭55.2.14 ）

業務部長が同会の発行する雑誌の購買者名簿を一時社外に持ち出しコピーし、競争関係にある転職先に譲り渡した。（窃盗）

⑥ 早大入試事件（東京高判昭56.8.25 ）

⑦ 新薬産業事件（1983検挙、東京地判昭59.6.15 、同6.28）

国立予防衛生研究所の技官が新薬承認申請に関する資料ファイルを一時持ち出しコピーし、製薬会社に売却した。（窃盗）

(2) コンピュータ情報

(a) プログラムの不正な持ち出し、コピー

① 新潟鉄工所事件（1983.2検挙、東京地判昭60.2.13 ）

コンピュータによる自動設計製図システムの開発を担当していた同社幹部従業員が、新会社設立を企て共謀のうえ、業務上保管していた同システムに関するプログラムの入ったフロッピーディスクを社外に一時持ち出しコピーした。（業務上横領等）

② 綜合コンピュータ事件（1984.6検挙、東京地判昭60.3.6）

ソフトウェアの開発販売を行う会社の課長とインストラクター等が新会社の設立を企て、標記会社の開発した新聞講読者管理システムのプログラムを無断で他のコンピュータに入力し販売。（背任）

③ 医師会事件（1984検挙）

同会臨床検査センター(社団法人)の元部長が、センター所長の管理する臨床検査業務処理システムプログラムの磁気テープをコピーした。(窃盗)

(b) 顧客リストの不正な持ち出し、コピー

④ 日経マグロウヒル事件（1971.2）

同者の定期講読者リストを入れた磁気ディスクが郵送業務委託先で何者かにコピーされ、売却された。(購入者を告訴の後、和解が成立し不起訴)

⑤ 日本チャリティプレート事件（1978）

民間福祉団体の総務部長が職務上保管している募金協力者名簿の磁気テープをコピーし売却した。（示談成立）

⑥ フジサンケイリビングサービス事件（1985）

同社から商品カタログの発送を委託されている会社の役員等が、保管している同社の顧客名簿41万5千人分を他のＤＭ会社に持ち込み、コピーをとって売却した疑いで取調べを受けた。（不起訴）

⑦ 軽自動車協会連合会事件（1986.4検挙、東京地判昭61.9.8）

協会課長等が、全国軽自動車1,200 万台に関する車両番号・形式、使用者の住所・氏名等を記録した磁気テープを一時持ち出しコピーし、ブローカーを介して売却。（窃盗）

⑧ 京王デパート事件（1987検挙、東京地判昭62.9.30 ）

同社の係長が職務上取扱っている顧客情報８万５千人分の磁気テープをコピーし、名簿販売業者に売却した。

⑨　総合法令事件（1988）

通信教育を業とする同社の元電算部幹部がコンピュータに保存されている受講者ファイルを他の媒体にコピーし、同人その他前役員等が新設したライバル会社に提供した。

(c) センター内での情報不正入手

⑩　近畿相互銀行事件（1981、大阪地判昭57.9.9）

同銀行を退職したオペレーターが休日にセンターに入り、データファイルに記録された大口預金者の口座番号、暗証番号を磁気読み取り機を用いて入手し、キャッシュカードを偽造して現金を窃取した。（有印私文書偽造行使、窃盗）

⑪　福岡銀行事件（1986検挙）

同銀行にシステム開発のため派遣されていたソフトウェア会社の技師が、センター内でテスト用端末機を操作し、テスト用元帳磁気ディスクに記録されている大口預金者の口座番号、乱数化された暗証番号等を抽出解読し、磁気テープつき通帳を偽造し、現金を窃取した。（有印私文書偽造、窃盗）

(d) 通信回線の盗聴

⑫　北海道銀行事件（1982.2検挙、札幌地判昭59.3.27 ）

電々公社技術職員が通信回線から銀行のＣＤオンライン取引データを盗聴録音し他人の暗証番号等を解読、キャッシュカードを偽造行使し、現金を引出した。（公衆電気通信法違反、窃盗）

(e) システム・ハッカーの侵入

⑬　ＫＤＤヴィーナスＰ侵入事件（1985.5）

(1)　外資系会社がＫＤＤのヴィーナスＰを利用し米国本社との間で在庫管理等の情報交換を行っていたところ、何者かにパスワードを盗用され、米国の10数社のデータベースからホビー情報等が引き出された。

(2) 東京の機械器具会社、データベース会社、大学研究所が西独、英、仏、スイスのハッカーによる侵入を受け、ファイルに“落書き”等をされた。（情報の流出はない模様）

⑭ 西独ハッカー事件

(1) 「トリスタン」事件（1985）

文部省の高エネルギー物理学研究所（筑波）の大型加速器「トリスタン」による国際共同研究に用いるミニコンピュータが、国際データ通信回線を通じ、西独ハッカーグループの侵入を受けた。（事務用ファイルの一部が壊されたり、落書きされたが情報の流出はない模様）

(2) 「ＫＧＢスパイ事件」（1989.3検挙）

西ドイツのハッカーグループがソ連の国家保安委員会（ＫＧＢ）の工作員にスカウトされ、欧米等の主要な宇宙、軍事、原子力関係のコンピュータシステムに侵入し情報収集を行っていたことが発覚したが、日本のシステムにも侵入したと伝えられている。

⑮ ＰＣ－ＶＡＮ事件（1988）

何者かが日本電気のＰＣ－ＶＡＮ（パソコン通信ネットワーク）にウィルス・プログラムを送り込んだ。そのプログラムを使うとウィルスは基本ソフトウェアに潜入し、次に使用者がＰＣ－ＶＡＮのホストコンピュータと交信した時、ウィルスは使用者のパスワードを、あらかじめ加害者の設定した指示に従い暗号化して、ネットの電子掲示板に書き込むようになっていた。

(3) その他（民事事件）

① ㈱エム・シー・エル事件（東京地判昭62.3.10 ）

同社はカナダ法人から精密鋳造用ロボットの製造技術の導入を受け、ロボットの日本における独占的製造販売権を許諾されていた。職務上その製造技術の秘密を知る同社従業員が、（ｉ）同社と競争関係にある新設会社

の役員に引き抜かれて秘密を提供するとともに、（ii）新設会社の依頼によりロボットの製造請負業者に働きかけ、他への納入禁止及び秘密保持の契約に違反して新設会社にロボットを納入させた。（（i）について従業員に秘密保持に関する債務不履行責任、（ii）について新設会社に法人の不法行為責任を認めた）

② 美濃窯業㈱事件（名古屋地判昭61.9.29 ）

同社の従業員でトンネルキルンの建設等の技術指導に従事していた者が、海外出張先で知り合った者から依頼を受け、同社の就業規則及び海外出張者に対する指示に違反して同社に無断でキルンの設計や技術指導を行い、技術知識を提供した。（雇用契約上の債務不履行及び不法行為に当るが、損害ないし因果関係の立証に問題があるとして請求を棄却）

③ ㈱ボンニー事件（大阪地判昭61.10.30）

同社はスウェーデンから導入したシステムに改良を加えて、婦人服縫製システムを開発し、工程部分の自動装置の試作を含む縫製装置の製作を請負業者に依頼した。

同請負業者は、システムの存在、仕組み及び使用方法等装置に関する情報を他に漏らさないという約束に違反して、その装置と技術要素の類似した装置を製作し子会社を通じて他に販売した。（秘密保持に関する契約書が作成されていないこと及び装置のうち新規性のある部分は請負業者の考案によるという理由で、守秘義務の存在を認めず請求を棄却）

2. 2　海外の事例

(1)　内部犯罪

「コンピュータ犯罪者の筆頭は、従業員となっている。システムにダメージを与える機会を最も多く持ち、特別の情報を手に入れやすいのも従業員であることから、従業員がコンピュータ犯罪に係わるおそれは、今後とも変わらないであろう。更に、従業員は財政的にも心理的にもコンピュータ犯罪に関与する動機を往々にして持ちやすい。コンピュータ・システムに対して悪質な損失を与えたケースは、従業員か、または前従業員が係わっていることが多い。」

（ブルームベッカー編 "Computer Crime Law Reporter"）

ズィーバーの「コンピュータ犯罪と刑法Ⅰ」の中で、コンピュータ・スパイとして紹介されている事例も、殆どが現職又は、退職した従業員の犯行である。次のような例が挙げられている。

(a) プログラムの不正な持ち出し

- ソフトウェア会社を退職してフリーとなったプログラマーが、在職中開発に係わった給与計算プログラムと同一内容のプログラムを、同社と同業の他社からの受注に応じ、納入した。
- 計算センターの元主任プログラマーが、在職中作成に携わった会計簿記及び賃金計算のプログラムを、自分と共犯者が設立した同業の会社に提供し、併せて顧客の引き抜きを図った。
- ソフトウェア会社のプログラマーが、自社のプログラムの入ったＭＴをコピーし同業他社に売却。
- 上記と同様の事例で、告訴が遅く、且つ会社の中で、加害者が自分の所持するＭＴに写し取ったのか、会社のＭＴに写し取ったのか不明のため、窃盗罪を適用できなかった例が報告されている。

なお、以上４件の被害者はいずれも小規模の企業である。

- ＢＯＡＣの従業員が自社の搭乗予約プログラムのコピーを同業他社

に売却しようとした（未遂）。

・　米国ＴＩＡＣ社のプログラマーが、地球物理学的計算及び石油探査の能率化のためのプログラムパッケージをコピーし、同業他社に売却。

(b) 顧客リストの不正な持ち出し

・　通信販売店の元従業員が、大口得意先のリストのコンピュータアウトプットを転職先に持ち込み、マイクロフィルムに撮影。

・　通信販売出版社のプログラマー兼オペレーターが全顧客リストの売却を企て、私用のＭＴにコピーしたが雇用者が計画に気づき未遂。

・　買収されたオペレーターが、商品として売られている運転免許証所持者の住所録の入ったＭＴをコピーして売却。

・　生保代理店の外務員が地方自治体地域計算センターの職員を買収し、学校を卒業し見習修業中の15～19才の青年の氏名、住所のリストを漏示させようとしたが未遂。

(c) その他の情報の侵害

・　産業スパイ事件としては、技術情報や顧客リストだけでなく、競争相手企業の原価計算、財務諸表、販売組織などの情報の不正入手が問題となるケースが少なくないとの指摘がある。（ズィーバー、前掲）

・　ＩＢＭ－日立事件で、日立が1981年に、ＩＢＭの企業秘密である新世代コンピュータ308Xのワークブック（設計仕様書）を入手したことが発覚したが、このワークブックは、ＩＢＭコンピュータ研究所に所属していた技術者が、ＩＢＭを退職する際に機密資料を持ち出さないという誓約書に違反して持ち出し、日立に売却したものである。

（フリーマントル「産業スパイ」）

・　シリコン・バレーの企業秘密を入手する手口として「実在しないポストの提供を広告して、ライバル会社からの応募者にしつこく質問し、相手方の機密を聞き出すというのが、競争関係にあるアメリカの会社がよくやるスパイ技術だ。」とされている。（フリーマントル、前掲）

(b) オンライン・システムによる犯罪

企業内オンライン・システムの発展によって、最近はミニコンとパソコンがオフィス内に普及し、ネットワークで結ばれるようになった。このような分散処理は、秘密情報へのアクセス可能なポイントを増加させにことになる。

- アメリカのハイテク企業の元従業員が、支社の端末から、他州にある本社のコンピュータにアクセスし、高価なプログラムを40本コピーした。彼は盗んだ資産を州間通商によって他州に移動させたとして起訴されたが、連邦裁判所は、電話回線を経由して送信される電子信号は資産とは認められないという理由で、この公訴を棄却した。

（ベックウェイ「ネットワーク犯罪白書」）

- カリフォルニア州パロアルトのソフトウェア会社のカストマ・サポート担当社員が解雇された２ヶ月後、家庭内のパソコンから会社のシステムにアクセスし、ソフトウェアの一部を破壊し、一部をコピーした。彼女は何らかの方法で従業員のアクセスコードを入手したと推測されている。（日経コンピュータ 1988.8.29）

(2) 外部犯罪 ―特殊な手口

部外者が特別な方法を用いて、暗証番号や口座番号その他の秘密情報を不正取得した例がいくつか報告されている。

- リフキン事件（アメリカ）……銀行の電信為替のバックアップシステムを開発した会社の下請業者が、連銀のコンサルタントを装って銀行の電子送金室に出入りし、他社の暗証番号を読み取ってノートにメモし、その預金を引き出してスイスのソ連取引所からダイヤモンドを購入した。
- ジュリー・シュナイダー事件（アメリカ）……電信電話会社の資材配送管理システムとセキュリティ対策を、部外者が、捨てられた書類

やテープの閲覧、雑誌記者を装ってのインタビュー等によって聞き出し、そのシステムを用いて資材を詐取した。

このような情報収集の手口はScavenging（くず拾い）の一例であるが、タイム・シェアリング・システムにおけるScavengingとして次の例がある。

- 石油会社の共同システムで、利用者の中の一社が、利用するたびにスクラッチテープ（一時記憶テープ）を磁気テープ装置に装着するよう要求し、書き込む前に同業他社がテープに残した秘密の地震データを読み取った。
- ＯＳの中には、テスト用補助機能として、複雑な許可手続を経ずに、コンピュータにアクセスできる臨時の仕掛け（Trap door…落し戸）が隠されていることがある。デトロイトでは、自動車工数名が商用タイム・シェアリング・システムの中で、パスワードを調べることのできるtrap door を発見し、時分割サービス会社の社長用のパスワードを入手して、企業秘密のプログラムのコピーを不正取得した。

その他秘密情報を不正入手する方法として，次のような手口が紹介されている。

- データをコンピュータの中で拾い上げたプログラムは、データを表す０と１の配列の順に従って、ＭＴ上で短い記録の読み書きを行う。犯人は向かい側の建物から窓越しに双眼鏡でテープの動きを見て、メモ帳に０と１を書きしるし、テープリールの動きを読み取る。
- コンピュータのプリンタが打ち出す音をカセットテープに録音し、おそ回しでリプレイする。

（以上Ｄ．パーカー「コンピュータ犯罪研究総論」）

- US.Sprint 事件（民事事件）……長距離電話サービスの供給を業とするUS.Sprint 社のアクセス・コードとカストマーの認識番号を、外部のブローカーが、有線通信を傍受し解読することによって不正取得

し売却した。

（ブルームベッカー編"Introduction to Computer Crime(2d Edition)"）

(3) 外部犯罪 ――システム・ハッカー

(a) 従来のハッカー

1980年代になって、パソコンをコンピュータ・システムの端末機として使用することが普及するうようになったが、これに伴い、若者がプロテクトを破ってコンピュータシステムに侵入することに快感を味わうという「ハッカー現象」が頻発するようになった。

- ニューヨーク・シティにある名門校ダルトン・スクールの学生グループが米国とカナダのいくつかのコンピュータに不正にアクセスしたとして起訴された。

（ブルームベッカー編"Computer Crime Law Reporter"）

- コンピュータゲート事件……1983年にミルウォーキーのティーンエイジャーのグループがデータ通信回線を経由して、ロスアラモス核物理研究所やセキュリティ・パシフィック銀行のシステムに侵入し、米連邦議会下院で査問を受けた。侵入の手口は、正規のユーザーがアクセスすると、そのパスワードを侵入者の手許にあるパソコンへ通報する仕掛け（trap）の入ったプログラムを送りつけることによって行われた。
- 同じく1983年には、19才の大学生がARPANET （米国防省のコンピュータシステム）に侵入し、さらにこれを中継点として、ノルウェーのNATOのコンピュータに侵入し、北大西洋の対ソ潜水艦作戦のためのコントロール情報を引き出している。
- 1985年には、ニュージャージー州の７人の少年がARPANET に侵入し、軍事通信システムのコードを不正取得したが、この中には通信衛星の位置を変更できるコードも含まれていた。
- 1985年には「ハンバーガー・カオス・ブラザーズ」と称する西独の

ハッカーグループが、西独のDESY研究所や、このシステムとつながりのある日本の高エネルギー研究所のシステム、その他のスイス、カナダなどのシステムに侵入した。

（以上　那野比古「侵入者ハッカーの挑戦」）

ハッカーがシステムに侵入することが可能となった方法としては、アクセスを代行するため預かったパスワードの流用や、パスワードを書きつけたメモの閲覧、人事異信録等から他人のパスワードを推測し、試行錯誤によって入手する方法、あるいは他人のパスワードを答えさせるスパイ・プログラムの使用など、多様な手口が用いられている。又、正規の研究者の間などでは、資料入手の必要上しばしばパスワードの貸し借りが行われるため、或るシステムに侵入しユーザーの電子メールの中味を覗くと芋づる式に多数の人のパスワードを入手できる等の実情が報告されている。（那野比古　前掲）

(b) 新しい現象

当初少数のマニアによって開発されたシステム侵入の手口、例えばスパイ・プログラムのテクニックなどは、BBS （電子掲示板）によって、伝播され、ハッカーの「大衆化」が起こる。パスワードや電話アクセスコードに関する情報を交換する「アングラBBS 」は全米に400 以上あるといわれている。（ベックウェイ、前掲）

このような傾向に伴って、当初の愉快犯的なタイプのハッカーだけでなく、侵入のテクニックを利益と結びつけようとするハッカーの出現が危惧されるようになった。1986年７月米ジョージタウン大学から発表されたレポートは、スパイ、テロリスト、過激派、マフィアとハッカーとのドッキングに深い懸念を示していると報告されている。

（那野比古、前掲）

- 1970年のコフマン事件……大学生のプログラマーが当初は腕試しのつもりで、タイム・シェアリング・システムに不正侵入し、ケンタッキー

州道路局の計画を入手したが、のちにそれを建設会社に売りつけようとした。

・　アラスカ・ノースロップ沖の海底石油の鉱区落札価格が、競売相手の企業により通信回線から盗聴（通信線にコイルを取付け電磁誘導を利用する）された事件。　（那野比古　前掲）

1988年3月に本格的な事件が報道されるに至った。新聞報道によれば、西独の3人のハッカーがスパイ容疑で逮捕されたが、3人は1985年に西独内で、ソ連のKGB の工作員にスカウトされ、コンピュータ・データと交換に金を受け取っていた。被害にあったのは、米国防省、NASA、原子力研究センター、仏伊共同の軍需コンツェルン、欧州共同の宇宙開発機構（ESA ）、原子力物理学の欧州合同原子核研究機関（GERN）、西独のマックス・プランク原子物理研究所などで、日本のシステムも含まれているとのことである。盗まれた情報は、コンピュータ利用による設計・製造システム（CAD/CAM ）のソフトウェアやマイクロチップスの設計図等とされている。又、東側に渡ったコード番号やパスワードの数は数千にのぼるともいわれている。（1988.3.3　朝日、日経、毎日夕刊）

又、コンピュータ・ウィルスによる事故が1987年半ばから急速な広がりを見せているが、1988年11月に世界的なコンピュータ・ネットワークであるインターネットで、コーネル大学大学院生が作成して流し込んだウィルス・プログラムによって、ネットワークにつながる6万台のコンピュータのうち6,200 台がデータ破損などの被害を受けるという事件が生じた。

コンピュータ・ウィルスの特徴は①自分自身をコピーするなど増殖力を持ち、他のプログラムに影響を与える②他のコンピュータ犯罪の手段となる③ネットワークでつながっているシステム全体に影響を与える。④一度ウィルスにかかると完全には治りにくい。⑤バックアップコピーにも影響与える ——などに整理できる。ウィルス汚染による損失は，調

査と修復のためのコストのほか、予想外に大きくなるおそれがある、とされている。

（富山茂　「高度化するコンピュータ犯罪〔米国最新事情〕①③」日経産業新聞1989.5/9,11 ）

(4) 組織犯罪

(a) 国際スパイ組織

次のような事例が報告されている。（いずれも米国の例）

（通信の傍受）

- ソ連の情報機関KGB が、ミサイル原子力潜水艦「トライデント」の主要な設計図の一部をファクシミリ通信の盗聴により入手した。

（ 那野比古、前掲）

- 「サンフランシスコのソ連領事館は、市を見おろす高台に建っている。領事館のアンテナはシリコンバレーに向き、コンピュータには機密通信を傍受するプログラムが入っている。ワシントンD.C も同じで、ソ連大使館のアンテナは、国務省とペンタゴンに照準を合わせている。もちろん、機密を傍受するためである。キューバのハバナにも、米国の衛星通信を傍受するためのアンテナがそそり立っている。」

（ベックウェイ、前掲）

サンフランシスコの領事館は、傍受した情報を暗号化し、上空を通過する自国の通信衛星に電波で吹き出す、という方法で送信した。

（フリーマントル、前掲）

（スパイの養成）

- 経済的に苦境にある人物、冷遇されている会社従業員等に経済援助を与えてスカウトする方法で、スパイの養成が行われている。
- ハーパー事件……経済的苦境にあったハーパーは、KGB にスカウトされ、「システムズ・コントロール社」の役員秘書兼記録係の女性と

結婚し、8年間にわたり軍事機密資料のコピーを持ち出させた。

- ホールデン・ベル事件……航空機や宇宙機器の大メーカー「ヒューズエアクラフト社」の従業員で個人的な負債を抱えていたベルをKGBがスカウトし、会社の機密情報を入手。
- クリストファー・ボイス事件……「TRW システムズ・グループ社」の冷遇されている従業員をスカウトし、同社の開発した、ソ連の弾道ミサイル発射実験を、アメリカの探査衛星からスパイするシステムに関する情報を入手。ボイスは報酬を麻薬買付けの代金に充てた。

（フリーマントル、前掲）

(b) マフィア

マフィアの関心は最近、ソフトウェアの窃取やコピー、自動支払システムの悪用、ハイテク・スパイなどに移ってきたといわれている。

プログラマー、オペレーター、システム・アナリストなどの情報処理関係者が、マフィアがらみの高利貸しに借金を返せないため、脅されて会社の高価なソフトウェアや秘密のデータを渡すというケースが少なくない。

又、最近逮捕されたインテル社の社員2名は、マフィアのコカインの密売組織のユーザーで、盗品のコンピュータチップとコカインを交換していた。ハイテク部品と麻薬の交換を専門とする大規模なマフィアの密売ルートがあるといわれている。

政府のデータベースからの不正入手の例もあり、麻薬取締局のコンピュータのプリントアウトが、マフィアの麻薬密売組織の手に渡っていた事例、連邦財務省の麻薬密売、盗難車などに関する取締情報システムが不正にアクセスされた事例が報告されている。

（ベックウェイ前掲）

米国のコンピュータ犯罪の増加理由の一つとして、強盗によるもうけの30倍ともいわれるコンピュータ犯罪のコストパフォーマンスの良さ

があげられ、米国では犯罪組織もピストルをコンピュータに持ち替えつつある。

又、犯罪によって得た資金を合法化するために、海外に送金し、これを還流させる方法をとる場合が多いといわれており、ここでもコンピュータが活躍している。　（富山茂、前掲②、1989, 5/10 ）

(5) 個人プライバシーの侵害

次のような事例が報告されている（いずれも米国の例）。

- 民間の調査会社員が、カリフォルニア州人材局の職員に賄賂を渡して、住民数人の個人情報をコンピュータでチェックさせた。

（ベックウェイ、前掲）

- 前保安官代理が許可なく犯罪記録ファイルにアクセスし、州のコンピュータ犯罪法で起訴され、数ヶ月の禁固刑を宣告された。
- ロスアンジェルスの郡警察の従業員が、コンピュータシステムに蓄積されている刑事訴訟関係の情報に繰返しアクセスしたとして、カリフォルニア州のコンピュータ犯罪法で起訴され，有罪判決を受けた。彼は入手した情報を私立探偵としての副業に使っていた。

なお、刑事訴訟関係の情報は、コンピュータ犯罪法に規定する「財産」の中に含まれると解釈された。

- 民間の保険調査員グループが許可なく医者のファイルを持ち出し、ファイルの中味をコピーして、ファイルは元へ戻すという事件が起きたが、コロラド州最高裁判所は、「ファイルの中味を永遠に奪う意思があったのではなく、ファイルの中の情報を探し出したにすぎない」という理由で、窃盗罪の適用を否定した。

（以上ブルームベッカー編、前掲）

なお、次のような指摘がされている。

「デスクトップ・コンピュータが普及したために、組織内外の多くの

人に関するデータを、誰でも目にすることができるようになっているが、従業員がこの権限を悪用しないようにするのは容易ではない。コンピュータの使い方を同じコンピュータでモニターしようとすれば、今度は従業員自身のプライバシーを侵すことになりかねない。労働組合は、コンピュータによるモニターには敏感に反発するが、一般に、コンピュータ・ファイルや他人あての電子メールをのぞくのはべつに悪いことではないという風潮がある。これは、なんとか変えていかなくてはならない。」　（ベックウェイ、前掲）

3．現行法による対応と問題点

3．1　現行法による対応

（行　為　の　態　様）	（刑　法　と　の　関　係）	（著作権法との関係）
（Ⅰ）保存または処理されている情報 (1)　［外形的な物の移動を伴う場合］ ①　情報を、記録している媒体ごと取る場合 ②　情報を記録している媒体を一時持出し、複写し、媒体は返還する場合 ③　被害者のセンターやオフィス内の端末にアクセスし、被害者の所有物である用紙、媒体にプリント・アウト、複写し、取る場合 (2)　［外形的な物の移動を伴わない場合］ ①　被害者のセンターやオフィス内の端末にアクセスし、画面で盗視し、または加害者の所有物である用紙、媒体にプリント・アウト、複写する場合 ②　通信回線を通じ加害者の端末の画面で盗視し、または加害者の所有物である用紙、媒体にプリント・アウト、複写する場合 （Ⅱ）伝送されている情報 ①　通信回線を伝送されている情報を、盗聴または、漏示する場合 ②　電波を傍受して漏示または窃用する場合	窃盗、横領または詐欺 同上（＊有罪判決例はあるが不法領得意思の成否等について疑義を持たれている） コピーについては、贓物罪は成立しない。 犯罪とならない 犯罪とならない ＊左記いずれの場合にも、行為者が部内者であるときは情報に対する職務上の関連如何により、財産的損害等の要件をみたせば背任罪が成立する。（但し要件充足に問題が多い。） （電機通信諸法との関係） ①　電気通信事業者の取扱中に係る通信の秘密を犯してはならない。秘密侵害は処罰される（電気通信事業法§4、§104、有線電気通信法§9、§14）。 ②　無線局の取扱中に係る無線通信の秘密を洩らし、又は窃用する場合は処罰される（電波法§109）。	＊　左記いずれの場合にも、情報が、著作権法で保護されるものであれば、著作権侵害罪が成立する。（著作権法§119） 著作権法で保護される電磁的情報とは、 ①　プログラムの著作物（学術等の範囲に属するもので思想を創作的に表現したもの。 但しプログラム著作物を構成するプログラム言語、規約、解法は対象とならない。） ②　ﾃﾞｰﾀﾍﾞｰｽで、その情報の選択又は体系的な構成によって創作性を有するもの。

情報の保護については、以上の諸法律のほか、①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律や、②特定の情報について不正取得あるいは漏示を処罰する法律がある。主なものを例示すれば次のとおりである（巻末参考1参照）

①の例

（公務員等公務に従事する者）

国家公務員法§100、§109（十二）、地方公務員法§34、§60、郵便法§9②、§80②、所得税法§243、法人税法§163、自衛隊法§59、§118
特許法§200

（上記以外の者）

刑法§134、電気通信事業法§4②、§90②、§104②③、有線電気通信法§14②、§15、電波法§109②、公認会計士法§27、§52、証券取引法§106、§156の11、§204

②の例

行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律§13、§25

日米相互防衛援助協定等に伴う秘密保護法

3．2　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。」

（62年度レポートＰ７、８　曽根委員）

（備　考）

1．本項の説明は主として、62年度当委員会レポート中の曽根委員「現行の刑法、特別刑法等による対処の可能性及び限界」に拠っている。

2．電気通信事業法§４、§104 による通信の秘密の保護と規律がどこまで及ぶかという点については、郵政省、ＮＴＴの見解をめぐって疑問が提起されている。前掲62年度レポート中、土屋委員（Ｐ47）及び渥美委員（Ｐ50～）の所説参照（巻末参考４に抄録）。

3．コンピュータ情報の不正取得、漏示を処罰する立法化の動きに対する消極論の論点を要約すると以下のとおりである（63年度委員会提出資料）。

○コンピュータ情報の不正入手、漏示

――「犯罪化」に対する消極論の論点

（１）不正行為の脅威とセキュリティ対策

①　コンピュータ・システムにおける不正行為の脅威は、過大評価されている。

コンピュータを特別視する風潮が、コンピュータ犯罪に対する幻想を助長している。

②　内部犯行が多く、犯人の割り出しはたやすいので、不正行為が頻発する可能性は少ない。

③　刑罰による企業秘密情報の過度な保護は、一部の大企業が恩恵にあずかるだけである。

④　基本的なセキュリティ対策によって、ほとんどの犯罪は防止できる。不正行為は、杜撰な管理など、システム設置者側の基本的セキュリテイの欠如によって生じる。

⑤　不正行為は、セキュリティ対策の充実によって防止すべきである。刑事法的保護は企業におけるセキュリティの怠慢を助長する。

（２）現行法による対応の可能性

不正行為は、現行の刑法及び特別法によって十分規制できる。

（３）「犯罪化」立法に関するその他の問題

①情報の不確定性、流動性、あいまいさは罪刑法定主義になじまない。

②処罰範囲の不当な拡大を誘発するおそれ。

（処罰範囲がハード、技術の展開と共に発展するおそれ、これまで不可罰であった行為が処罰範囲に取り込まれるおそれ。）

③研究開発を阻害するおそれ。

④転職の自由を抑制するおそれ。

⑤企業災害、公害の調査、内部告発を抑制するおそれ。

⑥保護法益をどのように考えるべきか、（財産犯か、秘密侵害犯か、企業秘密より個人プライバシーの保護を優先させるべきではないか等）

⑦情報の内容を重視すべきか、行為の態様を重視すべきか。

⑧国家機密保護罪に波及するおそれ。

⑨情報公開等個人の「知る権利」を機軸とする民主的コントロールを優先させるべきではないのか。

⑩刑事法以外の消費者保護対策を優先させるべきではないか。

⑪法による威嚇効果は期待されるか。

⑫捜査機関等による個人のプライバシー侵害に対する防護は用意されているか。

4. 刑法改正で積み残された理由

昭和62年の刑法改正については、前年秋から法制審議会における審議が開始されたが、その諮問は次のようなものであった。

「『電子計算機による情報処理組織の普及にかんがみ、緊急に刑法その他の罰則を整備する必要があるか。あるとすればその骨子を示されたい。』

右諮問は、……コンピュータに関連する不正行為が広範囲の問題にまたがるため、罰則整備の方向、内容について包括的な法制審議会の意見を求める形式をとっているものであるが、審議の便宜上、事務当局から、一応の問題点の整理として、刑事法部会において、次の五つの問題点の提示がなされ、おおむね、これらの諸点を中心に……審議が行われ、（62年）２月26日の法制審議会で答申案が採決された。

1　文書の多くが電子計算機用電磁的記録物上の記録に置き換えられつつある現状にかんがみ、これらの記録の改ざん、毀棄等につき、現行の文書の偽変造罪、毀棄罪等と同様の処罰規定を設ける必要はないか。

2　業務処理が広範に電算化された結果、電子情報処理組織に対する加害によって従来に比べてはるかに重大な業務妨害が生じ、かつこれが間接的には国民生活に大きな影響を及ぼす可能性の認められる現状にかんがみ、右加害を手段とする業務妨害行為に対し、法定刑を加重する必要はないか。

3　金融機関のバンキング・システムのように、単なる情報処理のみによって、かつ場合によっては人を介することなく機械的処理により完結する取引形態が増加しつつある現状にかんがみ、このような制度を悪用する財産的利得行為であって窃盗罪又は詐欺罪のいずれにも該当しないものにつき処罰規定を設ける必要はないか。

4　電子情報処理組織により処理及び保存される情報につき、その不正入手又は漏示を処罰の対象とする規定を設ける必要はないか。

5　権限なく他人の電子情報処理組織を利用する行為を処罰の対象とする

規定を設ける必要はないか。

刑事法部会においては、これらの問題点につき、既存の刑事法上、それぞれ的確な対応に困難があることはそのとおりであるが、第4点の情報の不正入手等については保護すべき情報の範囲、保護の程度等について検討を要する問題点が少なくないこと、第5点の無権限利用についてもどのような行為を処罰すべきか検討が必要なことが指摘され、第1点から第5点までを通観すると、第1点から第3点までは従来の刑法における文書偽変造・毀棄行為、不正な財産利得行為、業務妨害行為にそれぞれ対応する行為であって、従来の犯罪の分類等とも合致するものであるが、第4点と第5点の問題はむしろ新たな問題と考えられることからさらに種々の観点から研究を行うべきであり、差し当たっての緊急の立法的手当をするとすれば第1点から第3点について行うことが適当であるとする方向で意見の一致を見たものである。」

（古田佑紀・多谷千香子「刑法等一部改正法概説」
――警察学論集40巻8号）

「情報の不正入手又は漏示」の問題が見送られた背景には、昭和49年に法制審議会によって決定された「改正刑法草案」318条の「企業秘密漏示罪」をめぐって日弁連、一部学界等から強い反対があり、凍結状態となった経緯がある。

因みに改正刑法草案の「企業秘密漏示罪」とは次のような規定であった。

「第318条（企業秘密の漏示）

企業の役員又は従業者が、正当な理由がないのに、その企業の生産方法その他の技術に関する秘密を第三者に漏らしたときは、3年以下の懲役又は50万円以下の罰金に処する。これらの地位にあった者が、その企業の生産方法その他の技術に関する秘密を守るべき義務に違反して、これを第三者に漏らしたときも、同じである。」

「企業秘密漏示罪」に対する「批判の大要は、①本規定を個人の秘密を侵す罪に並べておくことの妥当性、②行為類型として部内者の漏示型を採用し

たことは、公害や消費者問題がおこった場合の内部告発の道を閉ざすことになる、③構成要件とくに「秘密」概念の不明確性、すなわち「企業の生産方法その他の技術に関する秘密」という場合の「その他の技術」とは何かが明らかではない、④犯罪主体としての「役員」、「従業者」にくわえて「これらの地位にあった者」という退職者についても適用をみとめ、さらに「秘密を守るべき法律上の義務に違反して」というきわめてあいまいな要件が付加され、これにより転職の自由は事実上閉ざされることになるということ、最後に、本罪がなによりも企業秘密保護にかんする国民的な議論もなされないまま企業利益優先のかっこうで提案されてきたこと、等があげられよう。」

（荒川雅行「企業秘密保護とコンピュータ犯罪」
――「犯罪と刑罰」1987年3号）

第２章　問題の検討

コンピュータ情報の不正取得や漏示を犯罪化する立法に対する消極論の論拠は、次の３つの部分から構成されている（Ｐ３０参照）。

第１は、不正行為の脅威は過大視されており、企業のセキュリティ対策によって十分防止できる、という認識である。

第２は、不正行為は現行の刑法及び特別法の解釈適用によって十分に対応できるという判断である。

第３は、犯罪立法が処罰範囲を不当に拡大し、又転職や報道の自由を妨げ、公害調査を抑圧する等の弊害をもたらすおそれがあるという不安である。

上記第１について、その認識の当否を検証することは、62年度の当委員会のテーマであった。本章１はその検証結果の要旨である。

上記第２について、その判断の当否を検証することは、63年度の当委員会のテーマの一つであり、本章2.１はその検証結果の要旨である。

当委員会としては、上記第１及び第２については、いずれも消極論の見解に対して反対方向に傾いており、したがって何らかの立法的対応を必要とする方向で、ほぼ合意に達しているものと考えられる。

本章2.２(1)はその要旨である。

立法化に当たって、上記第３の弊害を避け得るような犯罪類型を検討することは、当委員会の63年度及び平成元年度のテーマである。63年度においては、主として財産犯の方向で犯罪類型の検討を行った。その概要は本章2.２(2)に記すとおりである。

本章2.２(3)は、委員会の検討内容を事務局の見解を混えて整理し、今後の検討課題を摘記したものである。

1. 不正行為の脅威、セキュリティ対策等について

(1) 消極論の論旨

コンピュータ情報の不正取得や漏示を犯罪化する立法に対する消極論は、不正行為の脅威や、コンピュータシステムの「脆弱性」について、次のような見かたをしている。

① 「わが国の場合、通常……専用の『特定回線』が使用されており、外部の一般人の侵入は困難だとされている。」ハッカーによる侵入の事例はいずれも公衆回線によるものであり、「杜撰なパスワード管理などセキュリティ意識の欠如や、ごく初歩的なセキュリティ装置の不設置など逆にシステム設置者側の基本的セキュリティの欠如を露見させるものであったのである。」

又、外部者による犯行よりも内部犯行によるものが圧倒的に多いが、「ひとたびことが露見すれば、犯人の割り出しはたやすく、取り調べで自供を取り易いとの指摘がある。」とし、内部犯行についても、有効な部内監査や監督が行われていないことが指摘されている。

以上のような実態を直視すべきであり、「コンピュータの機能を過大評価し、コンピュータそのものを神秘化し、特別視する風潮が、かえって、コンピュータ犯罪に対する幻想を助長することになるのではないか。」としている。

（加藤敏幸「コンピュータ犯罪の実態と対応動向」
——「犯罪と刑罰」1987年3号）

② 「刑罰による情報の過度な保護は，結局は企業秘密の保護につながるのである。それもとくに国家権力と結びついた一部の大企業がその恩恵にあずかるだけであろう。」

「企業秘密を維持していくことが今後ますます企業存続のための条件となっていくであろうことが予想されるが、なによりもまず第1に企業自身

がそのための予防的戦略を確立しておく必要があろう。利潤の追及のみに目をうばわれ、セキュリティの確立といった直接的な利益と結び付かない点を軽視する企業の姿勢そのものが問題とされるべきである。」

企業秘密については、「たとえば、システム内の入退のチェックの強化、パスワードの工夫等でほとんどの防衛が可能だとされている。」会社の杜撰な管理システム、安全対策の不備は、警察庁のアンケート調査等からも明らかであり、「情報化社会のもつ『脆弱性』がいかに強調されようと、それをただちに刑罰による保護の対象とするよりも、むしろシステムのセキュリティ対策の確立がいっそう検討されるべきであろう。」

（荒川雅行「企業秘密保護とコンピュータ犯罪」――前掲）

(2) 消極論の検証

(a) 「不正行為の脅威は過大視されている」という見解

（上記①）について

「一昔前のコンピ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などが含まれるようになった。」（注） （62年度ﾚﾎﾟｰﾄP9、今野委員）

（注） ㈶日本情報処理開発協会が昭和63年１月時点でオンライン・ユーザー企業に対して行ったアンケート調査によれば（対象591社、回答率50％）、企業が重要な情報としてセキュリティ対策を講じまたは不正行為の潜在的脅威を強く意識している情報は多岐

にわたっている。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（各20％台）。

（62 年度レポートP64, P74）

「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。」（注）

（同　前）

（注）　なお、専用回線も安全ではないといわれている。ユーザー同士が他のコンピュータのセキュリティに関する情報を電子メールなどで交換しているケースがあるので、ひとつのシステムを破ると、「電子私書箱」の中味を覗くことにより、別のシステムに進入できる糸口が見つかる場合が多い。そのようにして、公衆網につながっているコンピュータが１ヵ所破られると、その先にいくら専用回線があっても、その専用回線の先のコンピュータまで侵入は次々と起こりうる（那野比古・前掲「侵略者ハッカーの挑戦」P71, P74）。

「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がりつつある。」

（同前　レポート P10）

一方オンライン・ネットワークの普及に伴い、企業の内部や取引先の端末から、重要な秘密情報にアクセスする機会や、その機会を利用できる人々の数も急速に拡大している。

そのような現象は、コンピュータ情報の不正コピーや窃用が人目につかず、行い得ることと相俟って、内部犯の場合にも犯人の割り出しは困難となってきている。

さらに、コンピュータによる情報処理は、業種の如何を問わず、又大企業だけでなく中小企業にも広がりつつある。

以上の観点からみると、「不正行為の脅威が過大視され、コンピュータ犯罪に対する幻想を助長している。」という認識は、オンライン・ネットワークの拡大しつつある状況においては、その妥当性に疑問があると思われる。

コンピュータシステムは、膨大な情報群を高密度に集積、整理、加工し、短時間で検索、伝送、出力、複写することを可能とした。人目につかず、きわめて軽いキー操作によって、多大の犯罪成果が迅速、的確に得られるという点に、文書に向けられた行為とは本質的に異なるコンピュータ犯罪としての情報犯罪の特徴がある。

コンピュータ情報の不正入手の分野では、組織犯罪やプロフェッショナルな犯罪、常習犯などが未だほとんど現れていない処から犯罪例は僅少であるが、ネットワーク社会への移行に伴い、不正行為の潜在的脅威が広がりつつあることは否定できないと考えられる。（注）

（注）　前掲アンケート調査によれば、情報に対する不正入手の脅威の程度をどのように意識しているかという問に対して、脅威の程度を「大」または「中」と答えた者の回答者全体に占める割合は、次のようになっている。

- 処理作業段階におけるアウトプット情報の複写……５６％
- 媒体の持ち出しによる情報の複写……４５％
- センター内の端末からのアクセス……４２％

これに対し、通信回線を経由するネットワーク犯罪のケースに関しては、

・企業内端末からのアクセス……４２％

・企業外端末からのアクセス……２２％

・通信回線の盗聴……２８％

・電波の傍受……１４％

となっている。

（62年度レポートP62, P71 ）

(b) 「不正行為は、企業のセキュリティ対策によって十分防止できる」という見解（上記②）について

(一) 「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。」

（62年度レポートP22, 池上委員）

「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。」

（同前　レポートP41, 小泉委員）

以上のように犯罪技術とセキュリティ対策との間に隙間を生ずることは避け難いとしても、パスワードの管理や情報媒体の受け渡し管理など、基本的なセキュリティ対策が杜撰であるという批判はしばしば耳にする処であり、

前記アンケート調査の結果をみても、企業におけるセキュリティ対策の実施状況は十分とはいえない。（注）

（注）　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。

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。

（同前　レポートP62 ）

基本的セキュリティ対策の充実は、今後も企業にとっての課題であろう。

唯、セキュリティ対策の充実は、不正行為の防止に寄与することは疑いないとしても、それのみによって不正行為を防止できるとは考えられない。それは次の理由による。

①　「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、技術的なセキュリティ対策の一律適用は、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。」

「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。」

（以上　62年度レポートP32, P33, P36 池上委員，小泉委員）

データ処理についての内部索制や、情報へのアクセス権限の細分化、情報媒体のライブラリからの持ち出しの管理、コールバック・システム、情報の

暗号化などをまともに徹底して行えば、業務の遂行は著しく困難となることが指摘されている。「ハッカーからシステムを完全に守る方法は、システムを回線から切離すことであるが、正規のユーザーも、オンライン・システムの利便さを一切諦めねばならない。」（注）

（注）　パスワード管理のルーズを示す例として、パスワードの貸し借りがしばしば挙げられるが、実際上の必要性から行われる例は少なくないといわれている。

（62年度レポートP15, 今野委員、那野比古、前掲書P72 ）

② 「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ことになるが、コンピュータシステムの構成要素が広範になればなるほど、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。」

「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……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。」

（62年度レポートP28, P33 池上委員）

前記アンケート調査によれば、年商規模、従業員数規模、コンピュータ投資規模のいずれで見ても、中規模企業の場合は大企業に比べて、セキュリティ対策の実施割合に著しい落ち込みが認められるが、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（同前レポートP64 ）。

以上のようにセキュリティ対策については、コスト面からも限界がある。

③ 如何に高度な防御体制を組み入れても、その仕組みを管理している要員の悪意に対しては有効な対策はない。

第１章２で例示したように、コンピュータ犯罪者の筆頭は、従業員等の部内者である。外部からの不正アクセスに対するどのように精密なセキュリティ対策も、その仕組みを管理している部内者を利用することに

よって崩される。

（二）　消極論においては、セキュリティ対策と犯罪立法とは、共に不正行為の防止という同一内容の機能を有し、一方が有効に機能すれば、他方は不要と考えられている。そのような観点から、犯罪立法は「安上がりの」セキュリティ対策であり、企業による自主的なセキュリティ対策の怠慢を助長するおそれがあるとされている。

セキュリティ対策と犯罪立法は、相互に関連するにしても、異なる機能を持つと考えられる。

セキュリティ対策は、総体的な事務処理の効率性や経済性とのバランスを考慮しつつ実施すべきものであるが、前記アンケート調査によれば、セキュリティ対策の効果としては、「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。」という点が主として期待されている。（前者は回答者の53％、後者は46％が挙げている。）

「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。」

（同前レポートP65 ）

プロによる犯行や内部の計画的犯行は、セキュリティ対策の射程外にあるといえるであろう。前記のアンケート調査によれば、犯罪立法は、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する者が回答者の33％を占めている。そのほか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が犯罪立法により認知されることが望ましいとする者が31％であった。

以上のように、セキュリティ対策と犯罪立法は、相互に補完し合う関係にあり、一方が他方に代替し、これを無用化する関係にあるとは考えられない。

2. 現行刑法の解釈及び立法的対応について

2.1 現行刑法の解釈

(1) 他人の保有する情報を、その情報が化体した有形の媒体を取り去ることによって得た場合に、「西欧諸国の法体系すべてにおいては、窃盗、横領の伝統的な規定を適用するのに何ら特別の問題を生じない。しかしながらデータの処理や伝達のシステムが、コンピュータ情報を速く、人目につかないで、(多くの場合遠距離通信設備によって) コピーできることから、伝統的な「情報媒体の窃盗」のほとんどが、(コンピュータ) 情報を媒体にコピーする行為にとって代わった。したがって、どの範囲まで無形の情報の純粋な取得に、伝統的な窃盗横領の規定が及ぶかという問題が生ずる。」

(ＯＥＣＤ特別委員会報告［ 147項］…巻末参考４)

日本の現行刑法には、情報自体の不正取得や漏示を処罰する規定はない。そこで窃盗、横領などの財物取得罪や背任罪の適用が問題となる。いくつかの下級審裁判例は、情報の化体した媒体をコピーのため一時社外に持ち出す行為について、財物取得罪の成立を認めている。

財物取得罪の成立には、客体の「財物性」と「不法領得の意思」が問題となる。この点について、(文書のコピーの例ではあるが) 建設調査会事件 (東京地判昭55.2.14) 、新薬産業事件 (東京地判昭59.6.15 、同59.6.28) は、「有形物である媒体に価値ある情報が化体されていることを捉えて、その両者を合せたものとして客体の財物性を理解した上、財物としての価値がそれに依存する情報の排他的・独占的利用が害される点で、一時持ち出しにも不法領得の意思が認められるとするものといえよう。」

(中森委員、「法学教室」1985年No.61)

(注) なお新潟鉄工所事件 (東京地判昭和60.2.13) の場合は、コンピュータ・プログラムの化体した磁気テープ等の一時持ち出しコピーについて、業務上横領罪が適用された。本件の場合、有罪とする結論は以上の先例に沿

ったものであるが、「結局のところ『許可なしにコピーすることは許されないものであった』という点が、不法領得の意思、横領罪を認めるについて決定的なものとされているように思われる。」　（中森委員、前掲）

次に背任罪の適用に関しては、「事務処理についての任務違背」という要件で、行為主体の範囲が絞られるため、例えば技術開発に当ったエンジニア等は対象からはずれる場合が多い。また本人に「財産上の損害」を加えるという要件については、被害者である企業が情報の流出により、競争上不利になるおそれがあるというだけでは損害の発生を認め得ないとする見解がこれまで刑法学界では有力であり、背任罪を適用できるケースは極めて少ないとみられている。（注）

（注）東洋レーヨン事件（神戸地判昭56.3.27 ）では、加害者が担当事務の処理のため入手した情報ではないという理由で背任罪が否定された。綜合コンピュータ事件（東京地判昭60.3.6）では、会社が商品として販売するコンピュータ・プログラムを、加害者が無断で他社の扱うコンピュータに入力することにより、会社に平均販売価格相当の財産上の損害を与えたものと認定し、背任罪の成立を認めたが、このような理由による「財産的損害」の認定には疑問があるとされている。　（中森委員、前掲）

(2) 上記の建設調査会事件や新薬産業事件の裁判例で示された客体の「財物性」及び「不法領得」の理由づけについては、学界で肯定する見解も少なくないようであるが、63年度における当委員会の討議では、次のような批判が提起されている。

① 客体の「財物性」について

裁判所の解釈によると、1枚の紙に情報が化体されている場合、情報全体の財産価値がその紙に含まれると考え、1枚の紙の窃盗を認めている。情報の窃盗という実質を、財物の窃盗という犯罪類型の中に、何とかやりくりして押しこめているのが実情で、刑法の適用という観点からみると問題である。そこまで解釈により刑法を押し曲げて処罰するのは行き過ぎであり、相応の立法的な裏づけをすべきである。

② 「不法領得」について

「不法領得」は、不法に利益を得ることと、被害者の利用可能性を奪うことを本質的特徴としている。被害者の利用可能性を奪うことが「不法領得」の成立に必要とされるのは、財物の窃盗と使用窃盗を区別し、使用窃盗を処罰対象から除くためである。

媒体を一時社外に持ち出し、化体されている情報をコピーして不正に取得し、媒体は持ち主に返還する場合、被害者がその情報を利用する可能性は奪われない。

そのような場合にも「不法領得」が成立すると考えるのは、不法領得概念の不当な拡大である。そのように解釈で不法領得概念を拡げることを認めるならば、やがては「所有者の如く」ふるまったという理由で、解釈により使用窃盗が犯罪にとり込まれる危険を生ずるであろう。

西欧諸国では、不法領得に関する基本的な定義づけや厳格な概念設定を基礎として制度を構築しているから（注）、日本の国内法の適用で、解釈により不法領得概念を拡げてゆくと、国際的に法制度が斉合的でなくなるという問題が生ずる。とりわけ情報については、今後の国際交流の進展を考えると、法制的な基本概念に違いがあるのは問題である。

（注）ＯＥＣＤ特別委員会報告［ 148項以下］…巻末参考４参照）

③ 以上のように考えると、現行刑法の解釈で財物取得罪の規定を疑問の余地なく適用できるのは、財産価値ある情報を媒体ごと持ち去る場合だけであって、それ以外の場合、例えば上記の媒体を一時社外に持ち出しコピーする事例や、センター内で情報を被害者の所持する別の媒体にコピーして持ち出す事例（注）に窃盗罪や横領罪を適用したのは苦しまぎれのこじつけであろうと批判されている。

（注）被害者の所持する感光紙にコピーして持ち出した事例として、大日本印刷事件（東京地判昭40.6.26 ）がある。

2.2 立法的対応

(1) 立法的対応の必要性

(a) コンピュータ情報の不正取得、漏示については、現行刑法による対応で充分であり、それ以上に敢えて立法措置を考える必要はないとの見解が当委員会の外部にあるが、当委員会としては、（コンピュータ情報とその他の情報を区別するか否かという点は別として）何らかの立法的対応を必要とする見解が支配的であると考えられる。

その主たる理由の第一は、現行刑法の財物取得罪の適用を前提とする限り、処罰の可否が有体物である媒体の移動の有無により左右されてしまうという点である。

上述の裁判例でも、一時的にせよコピー目的で媒体を社外に持ち出したこと、あるいは被害者の所持する媒体にコピーして持ち出したことを捉えて、窃盗、横領の決め手の一つとしている。

ネットワークシステムの拡大、通信回線による情報へのアクセス機会の増加、情報処理の大衆化といった状況を考慮するならば、そのような取扱いが不合理であることは明白である。

第二は、財物取得罪を適用するに当って、解釈による不法領得概念の拡大という操作を行わざるを得ず、そのことが、刑法全体の斉合的な解釈を歪め、また不法領得概念に関する国際的な理解にも抵触するおそれがあるという点である。

第三は、情報犯罪に処罰の間隙を生ずることは、情報の国際交流の妨げとなるおそれがある点である。

(b) なお委員会では、上記に関連して次のような指摘が行われた。

- 情報の不正取得や漏示の実例が些程増えていないのは、システムに侵害するという困難に挑戦して、情報窃取を莫大な利益に結びつけようとする者が少ないためであろう。

  会社の経営者は、自分のシステムには侵入されないと思っており、安全

対策もなおざりにしている。

- しかし最近の傾向として、コンピュータシステム内に重要な情報が常駐するケースが増えており、一方警察庁のアンケートでは、技術者の大半はシステム内の情報を覗くことに余り罪の意識を持っていない。

アメリカでは、ハッカーもかつてのように知的な青年というイメージはうすれ、大衆化しつつある。本人に技術的知識がなくても、他人を利用してシステムに侵入することは可能であり、組織犯罪グループによる犯行も生じている。

アメリカの事例は早晩日本にも波及するおそれがある。

- 企業内部でも、コピー目的による媒体の社外持ち出しだけでなく、センター内でデータ類（電磁的記録だけでなく、プリントアウトされた資料を含めて）をコピーし、持ち出す等の危険は、従業員の引き抜き、転職等の増加に伴い増えることが予想される。
- 情報の不正取得や漏示の潜在的脅威は軽視できない状況にある。

アメリカでは、不正行為に対処するため、連邦法や州法レベルでさまざまな立法的な手当てが行われており、いまそれらをまとめて、斉合性を持たせることを考える段階に来ている。

西ドイツでは、日本のようにコンピュータによる情報処理が普及していないが、それでも今後起り得べきケースを洗いざらい想定して、何とか対処するため法的措置を講じようとしている。

- 不正行為については、民事責任で対応する方法も考えられるが、民事責任が機能するのは大企業同士の場合であって、その他の場合は逃亡したり会社を潰してしまうので、民事責任は機能しない。

特に組織犯罪に対する抑止力は、刑事責任によらなければ期待し得ないのではないか。

- 組織犯罪、不正競争関係の犯罪などに、諸外国は提携しながら対処しようとする動きが出ている。

情報の領域では世界的なネットワークに入りながら、日本でだけ情報侵害が犯罪にならないという状況は問題であって、外圧により日本の国内法のあり方も影響される可能性がある。情報侵害に対して刑法的な保護を講ずるため、どのような犯罪類型を定めれば国際的な付託にこたえられるか、将来展望を考えながら検討する必要がある。

- 諸外国の対応に比べると、日本は「裸の王様」のようだ。それでいて事件が起ると、明治40年の刑法の解釈で何とか有罪にしてしまうのだから、こんな怖いことはない。

(2) 処罰対象とする犯罪類型

コンピュータ情報の不正取得や漏示に関して処罰対象とする犯罪類型については、代表的なものとして次の二つの方向が考えられる。一つは財産保護の見地から、財産的情報の不正な移転を犯罪とする「財産犯罪」の方向である。他の一つはインフラストラクチャーとしての情報処理システムの完全性を保護するという見地から、コンピュータシステムの無権限アクセスを原型として情報侵害を捉える「システム侵害罪」の方向である。

前者は在来型の犯罪概念の展開であり、後者は新しい犯罪概念の創設となる。日本では判例の中に、無形の情報を財物の中に含めて盗犯の対象にしようとする傾向が強く現れており、一昨年の刑法改正も在来型の展開として行われたという経緯もあるので、当委員会としては63年度において、まず財産犯の方向から立法論的な検討を始めることとした。(注)

(注) 財産犯の代表的な類型については、P61「犯罪類型の比較」参照。但し同表のうち「西ドイツ刑法§202A」は財産犯ではなく、秘密侵害犯である。なおシステム侵害犯の諸類型についてはP63～68「犯罪類型の比較(アメリカ州法)」参照。

(一) 財産犯的な方向での代表的な立法案として想定されるものは次の三つである。

(A) 「財産価値のある情報の化体された有体物は財物とみなす」案

この案は、媒体それ自体の価値がほとんどなくても、その中に財産価値のある情報が化体している場合には、その情報を含めたものとして媒体の価値を評価し、財物として盗犯の対象にするという案である（イギリス方式）。

判例が解釈により、実質的な情報窃盗を有体物である媒体の窃盗に偽制し、不法領得概念を拡大しているのは問題であるから、上記の規定を明文化して法的な裏づけをつくるというのがこの案の狙いである。

但し、この案は窃盗・横領罪に関する判例の解釈を立法的に追認することにとどまるので、媒体の移動を伴わない場合、すなわちセンター内で加害者のフロッピーシートに情報を写し取る場合や、端末から遠隔操作で情報をプリントアウトする場合は犯罪とならない。

(B) 「有体物に化体された財産価値ある情報は財物とみなす」案

情報が有体物に化体されているということは、情報の保有者がその情報を有体物に化体することによって管理可能としている状態であると考えられる。そのような状態にある情報自体を、財物とみなして盗犯の対象にするという案である（イギリス方式の展開）。

この案によれば、有体物、すなわちtangibleな媒体に化体されている情報（コンピュータ内のメモリに記録された情報も含まれる）については、媒体の持ち出しの如何にかかわらず、情報それ自体を不正に取得したり漏示することが窃盗、横領罪となる。したがってA案の場合のような処罰の間隙は生じない。

なお盗犯が成立するためには、情報を紙にプリントアウトする、フロッピーシートに複写する、画像をカメラで撮影する等、情報を機械的に直接他の媒体に固定する方法によって取ることが必要で、ディスプレイに映し出して記憶したり、メモする場合は盗犯にならないと解されている。

次に盗犯の成立を認めるに当って、被害者の許にオリジナルな情報が残

ることを不法領得との関連でどう考えるかという点については、「被害者の媒体に化体した財物としての情報を、複写により加害者の媒体に財物として化体させることは、被害者の許にオリジナルな情報が残っていても、情報に対する被害者の支配を一部排して、その情報を加害者の占有状態に移したといえるのではないか」として、不法領得の成立が説明されている。

(C) (1988年) 刑法学会報告案

「規定案

第一　職務上知り得た他人の財産価値を有する技術上または営業上の秘密情報を窃用（その情報の本来の用法に従って不正に利用し、それにより当該情報の有する財産価値を侵害）すること（5年以下の懲役または罰金）。

第二　職務上知り得た他人の財産価値を有する技術上または営業上の秘密情報を窃用の目的で漏示すること（3年以下の懲役また罰金）。

第三　他人の財産価値を有する技術上または営業上の秘密情報を窃用の目的で不正に取得すること（3年以下の懲役または罰金）。」

（注）この案は、昭和63年 5月28日日本刑法学会において「財産的情報の刑法的保護」と題する共同研究の一部として報告されたものである。

概要については、末尾参考4の当委員会における西田委員の講演要旨参照（P123）。

この案は、「有形物に化体された無形的情報を刑法 235条の［財物］の中に含めて、あるいは拡張して処罰してゆこうという方向が判例の中にも色濃く出ているが、このような判例の方向は財産犯規定のあり方として健全なものとはいい得ないものである。」（西田委員、前掲）という認識に基づき判例の動向に歯止めを掛けるとともに、併せて通信回線を経由して情報を盗み出すというような財物性を超えた情報の侵害に対処するため、新たな立法案として提示されたものである。

この案のポイントは次の二つに在ると考えられる。

① 従来判例では、政党の指令通信が記載された１枚の紙の窃取が窃盗罪とされている。政治的な意味しかない文書を、財産価値あるもの、すなわち「財物」とみなして窃盗罪に入れてしまうのが裁判の実態と思われる。

この案は、「財産価値ある情報」の範囲を絞ることによって、そのような判例の傾向を立法的に制限することを意図している。すなわち情報の財産価値を情報を取る側から捉えると、処分してカネになりそうな情報であれば凡そどのような情報でも財産価値があることとなる。この案は、情報を取られる側にとって、情報の流出が財産価値の喪失を意味する場合に限って、その情報の財産価値を認める。それによって、国家機密等の政治的な秘密情報の侵害が、財産犯の名のもとに裁判所の解釈で安易に処罰されることを抑制しようと試みている。

② 「財物移転罪は、有体物の占有によって、その権利者が有している具体的な利用可能性を保護の対象としている。」情報が不正にコピーされた場合は、「情報それ自体はなくならないので、利用可能性は侵害されない。その場合は、情報が拡散したにすぎないのであって、その侵害の実体は情報を独占的に利用し得る地位という経済的利益が侵害されたことにほかならない。」「情報の持つ特殊な性質と現行法における財物移転罪との相違点を考慮すれば、新たな立法によって対処すべきであるという結論が導かれる。」（西田委員、前掲）

以上の理由により、財物移転罪ではない財産犯として、財産価値ある情報の不正取得・漏示罪が提示されている。

（二）上記の立法案ＡＢＣの構成要件に内在する主要な問題として、当委員会の討議で次のような問題が指摘された。

① 「財産価値ある情報」について

立法案に共通の問題として、客体となる「財産価値ある情報」の概念

が不明瞭である点が指摘された。

情報の財産価値は、開発や購入に要した原価によって計量し得る場合には比較的明瞭である。しかしプログラムやデータには、利用者によって価値が生み出されるという性質がある。そのように効用価値の観点を入れてゆくと、「財産価値ある情報」の概念は捉え難く拡がる可能性があり、限定的な概念としての意味を為さないのではないかという点が指摘された。

上記C案は、そのような客体概念の拡散に絞りをかけるために、その情報が被害者にとって財産価値があることを要件としているが、それは客体の範囲の限定となり得るのかという点が疑問視された。実際問題として、被害者にとっての財産的損害を計量することは難しいが、反面外交・国防上の秘密情報であっても、被害者の側で財産価値を認め得るケースが相当あると思われるので、C案が意図するように、外交・国防上の秘密情報を客体から排除できるかという点についても疑問があるとされた。またC案の場合は、A案、B案のように、客体に関し媒体に化体された情報という限定がないので、被害者の側で財産価値があると考えている抽象的な企業秘密 —— トレード・シークレットなどが歯止めなく入ってくるおそれがあるのではないかということが問題点として指摘された。

一方企業の保有する秘密情報の中には、経営情報や取引先の情報、個人情報などで財産的情報とはいい難いものもあり得るが、その暴露等による損害を看過してよいのかという問題も指摘された。

② 「不法領得の意思」及び「窃用の目的」について

上記A案、B案に共通する問題として、「財物とみなす」という規定の仕方は、無形的情報を財物概念の中にとり込むことによって盗犯の対象とする試みであるが、盗犯の要件である「不法領得の意思」の適用に関して無理を生ずるのを避け難いのではないかという問題が指摘された。

〔因みにイギリスでは、1968年の窃盗法は「財産」に無形財産を含むとしたが、Oxford vs. Moss事件において控訴裁判所は1979年に、「永久的に他人からそれを奪う」故意を要件とする特定の条文は、有形物についてのみ適用される、という理由で、機密情報 —— 例えば学生が不正に取得した大学の試験問題 —— は、盗犯の対象にならないと判示した（ＯＥＣＤ特別委員会報告［ 150項］…巻末参考４）。〕

上記Ｃ案は、情報の特殊性を考慮し「不法領得の意思」を要件とする財物移転罪に代えて、「窃用」を目的とする財産的情報の不正取得・漏示罪を提示している。

「窃用」という概念は、「その情報の本来の用法に従って不正に利用し、それにより当該情報の有する財産価値を侵害すること」と定義されており、被害者の許に情報は残るが、その価値が毀損されるという点で、毀棄的な要素を含む概念であるが、唯、「窃用」という概念は漠然として捉え難いという問題が指摘された。すなわち、「窃用」の目的はどのようにして把握できるのか。「窃用」は、情報の不正利用と、それによる当該情報の財産価値の侵害を意味すると定義されているが、情報の財産価値の侵害はつかみどころがないのではないか。取得したあとの情報の窃用は秘密裡に行われ、場合によっては相当永い時間を経て行われることもあり得るという点をどのように考えるのか、といった疑問も出されている。なお「窃用」という外国人に理解し難いと思われる、あいまいな概念を用いることは、情報処理の国際化が進みつつある現在、適切ではないとの指摘もあった。

(三)　財産犯として位置づけられる上記Ａ～Ｃの案については、以上のような問題点の指摘が為されたが、そのような問題を意識しながらも、これを評価する見解も示されている。

すなわち「財産価値ある情報」という概念が明確さを欠くことは否定し難いが、この程度のあいまいさは現実の解釈論の中でこなしていけないわ

けではない。財産的な被害の大きな不正行為を抑止するという立法化の主目的からみて、多少の問題はあるにしも、まず客体を財産的な情報として抑えることが先決であるとの意見が示された。

次に「財物」及び「不法領得」概念の類推による（上記A案、B案）か、「窃用」概念による（上記C案）かについても、それぞれに賛意が示されている。

前者の意見としては、伝統的な財産犯へのなじみやすさ、国際的な理解等の観点から、上記A案またはB案の方式で刑法に規定し、これによって保護できないものは、コンピュータシステムを保護するための特別法等によって対処するという考え方がある。

後者の意見としては、情報の不正取得や漏示に関しては有体物に関する従来の不法領得や窃取の概念を超えた新しい行為概念を設定することが必要で、「窃用」という概念はその一つの試みであり、種々問題はあるにしても、事例の積み上げによってリファインされるのではないかとされている。

（四） 前記のほか財産犯としての立法を考える方向自体に対しては、次のような批判的見解が示されている。

① 財産犯的な把え方は、客体である情報を財産的な情報と非財産的な情報に分けることを前提としているが、そのように分けること自体に問題がある。

有体物とちがって情報の場合は、情報の財産価値が、利用の仕方によって左右される等の事情で捉え難いうえに、情報の不正流出によってもたらされる損害も、流出した情報の使われ方や周囲の状況によって、財産的であったり非財産的であったり、あるいは損害が生じないということもあり得る。

例えば、企業の保有する個人情報が不正に流出した場合は、使われ方しだいで、情報管理者である企業に財産的損害を生ずることもあれば、情報

主体である個人のプライバシーが侵害されることもある。企業の経営情報が不正に流出する場合も、状況により、使われ方しだいで、企業の事業計画の遂行に支障を来す等財産的損害に直結することもあれば、企業の信用低下など、必ずしも財産的とはいえない損害につながることもある。

以上のような情報の特殊性は、客体の中に含まれている財産価値が、客体の不正流出によって失われ、財産的損害を生ずるという、有体物に関する財産犯の図式になじまないのではないかという疑問を抱かせる。

そのような疑問もあって、立法の方向としては、財産犯的なアプローチではなく、コンピュータ・システムへの不法な侵入を切り口とし、財産価値ある情報の侵害や業務妨害等を行為の結果として捉えるべきではないかあるいは、客体となる情報の質だけでなく、情報に対する管理の仕方や、情報へのアクセス、情報の伝達等行為の面からの検討が必要ではないかという指摘が為された。

又、情報の保護は、財産価値の面からのみ、一元的に考えるのではなく、例えば、情報の財産価値とコンピュータ・システムに関する経済利益、個人のプライバシーを分けて、それぞれを別の法律で保護することを考えてはどうかという意見も示された。

② 財産価値のある情報の不正取得や漏示は、即当罰性ありとする考え方は問題である。

現行法では、無体財産権制度により、情報の中で、一定の手続きをとったもの、あるいは創作性のある情報だけが刑法的にも保護されており、その他の情報は財産価値があっても、権限なき取得や提供は、原則的には犯罪とならない。

それを刑法でいきなり処罰対象にすることは極めて問題であり、情報の利用に際し、いちいち情報の帰属主体の了解を得なければならないということになると、情報化を畏縮させる結果ともなろう。

したがって刑法的な保護を行う場合は、その情報に対して特別な管理が

為されている場合に、それを侵害するといった行為態様の不正によって、絞りをかける必要がある。

③ 近年ハッカーの跳梁が目立つようになり、パソコンにプログラムを組み入れ、多数のコンピュータにアクセスを試みるとか、コンピュータの作動に伴って生ずる電磁波を傍受する等、情報入手の意図は不特定で、アクセス手段の問題性が著しいという現象も現れている。そのような場合は、情報の質よりも行為の面を重視すべきではないか。

④ その他窃盗ないし財産犯的な類型に捉われず、他のパターンを考えてもよいのではないかとういう指摘がいくつか為されている。

例えば、毀棄罪、業務妨害罪的な考えを入れる。あるいは、被害者に生じた財産的損害に対応する刑罰を考えるのではなく、情報を不正に入手したことによって不当に利益を得たことに対応して処罰するという発想もあり得る、とされている。

（五） 財産犯的な方向での検討に関連して、その他次のような討議が行われた。

① 情報に関するセキュリティ対策について

客体となる情報に関し、不正アクセスを防止するためのセキュリティ対策が講ぜられていることを、犯罪の構成要件とすべきかという点については、次のような意見があった。

(a) 秘密侵害罪として構成する場合は、情報についてのセキュリティ対策が重要な要件となる。これに反し、財産犯としての窃盗罪の単純な展開で考える場合は、他人の所持管理している（例えば建物の中にある）情報に権限なくアクセスするという要件だけで充分であり、セキュリティ対策の実施されていることを要件とする必要は、本来的にはない筈である。それにもかかわらず財産犯の成立に、情報の秘密性ないしセキュリティ対策が必要だという考えがあるとすれば、その実質的理由は何かが問題となる。情報の財産価値が不明確であることと関連して、情報の財

産価値を担保する役割を持つとも考えられる。

(b) セキュリティ対策を要件とする場合、一定水準以上のセキュリティ対策を要求することは問題である。セキュリティの水準については、パスワードによる管理だけではなく、プログラムの作成手順等についてもさまざまな方策と考え方がある。通産省は安全対策基準を制定しているが、安全対策に対する考え方は、個々の企業の特性によって異なる。セキュリティ対策をどのように評価し、投資するかは、それぞれの企業の判断に依存している。セキュリティ対策が客観的に一定水準以上であるか否かを判断することは非常に難しい。

② 漏示について

前記立法案A、Bの場合は、財産価値ある情報が有体物に化体されていることを前提として、その媒体、あるいは情報が財物とみなされるので、その情報の漏示については横領罪が適用される。これに反しC案の場合は、財産価値ある技術上又は営業上の情報を窃用の目的で漏示することは、その情報が媒体に化体された情報であるか否かを問わず、犯罪となる。

漏示については次のような意見があった。

(a) 記憶の中にある重要な技術情報などを口頭で漏示することも、高度な専門家同士の場合には可能であるが、そのように当人の頭の中にある情報の漏示を犯罪とすることは、どう絞りをかけても問題があろう。例えば、契約による守秘義務の存在が前提となるが、その義務は離職後どこまで及ぶのか。その人独自の専門的なアイディアで全体的な技術開発に寄与しているものを漏らす場合と、会議などで他人から聞いて記憶している情報を漏らす場合とで違いがあるのかといった問題が絡んでいる。

(b) 前記A案、B案のように、媒体に化体されている情報を他の媒体に写し取って漏示することを要件とするときは、処罰範囲は限定されるが、それだけで当罰性があると考えるのは問題ではないか。

契約等による守秘義務が要件になるとしても、情報の内容に関し、企

業サイドでの重要性だけで、刑法的保護に値するとは限らず、また当然守秘義務契約の退職後の効力も問題となる。

(c) 刑事責任よりも民事責任を優先させるべきではないか。

なお、刑事、民事のいずれにせよ、責任追及によって、同業他社への転職や独立が、がんじがらめにされるのは、時代の趨勢に逆行するのではないか。

(d) アメリカでは、企業内の秘密情報に関しては、従来永年にわたり、従業員との契約や就業規則、無体財産権等さまざまな方策で保護されて来た経緯がある。コンピュータ・システム内の情報やトレード・シークレットを刑法的に保護する立法を行うに当たっては、従来の諸方策との間に整合性を保つよう細心の配慮が払われた

日本の企業においては、秘密保持の契約慣行も乏しく、一般的な忠実義務だけで運営されてきたから、情報の無断持ち出しを処罰する立法が突然行われると、社会的な混乱を生ずるおそれがある。

(六) 立法化に当たって、刑法に規定するか特別法に規定するかという点に関し、次の意見があった。

① 刑法という国の刑罰権行使の基本法的なものに規定する場合と、特別法に規定する場合とでは考え方、内容に違いが出るであろう。特にプライバシーの保護に関しては、大きく違ってくると思われる。

② 情報の不正取得や漏示を犯罪化する規定を刑法典の中に入れることについては、外部に強い反対があり、又人間の自然的な反倫理行為を基本として法文化している刑法の中に、新しい社会現象であるコンピュータ関連犯罪の、しかも一昨年の刑法改正で積み残された部分に関する規定を入れることについては心理的な抵抗感もあって、当委員会で刑法改正の提案をしても、法務省は積極的に取り込もうとしないのではないか。

プライバシーの侵害やコンピュータ情報の侵害に対処するための特別法というような行政刑法の形で規定する方が可能性としては大きいが、日本

の実務の特殊事情として略式命令による罰金で処理されるケースが多く、犯罪の予防効果という点に問題がある。

（但し、行政刑法の機能とうい点に関しては、例えば著作権法の場合、レンタルソフト業界に対する強制捜査が行われて脱法行為も抑制され、刑罰規定が社会的に影響力を持っていることが指摘されている。）

③　前記のような事実上の難しさはあるにしても、考え方としては、コンピュータに関係する犯罪という形で刑法典に規定するという選択もあり得る。その場合は、社会的法益に対する罪として規定する形もあるが、そのほか、別の章を設けるという方法もある。諸外国で、後者の方法を採用している例があるのは、そうすることによって、刑法的な保護の対象をコンピュータ・システムにおいて貯蔵され、あるいは伝送される情報に限定し、トレード・シークレットのような抽象的な企業秘密にまで、処罰対象が拡がることを阻止しようという配慮があるからである。

日本では、既存の刑法の財産犯的な発想でどこまでカヴァーできるかということを考えているため、トレード・シークレットのような諸外国ではコンセンサスの得難い情報の保護を簡単に容認する意見が出る一方、当然保護されるべきコンピュータ内の情報が対象からはずれるという矛盾を生じている。

〔コンピュータ情報の不正取得・漏示〕　犯罪類型の比較

構成要件等 ＼ 犯罪類型				判例〔下級審〕（窃盗罪、横領罪の解釈）	「財産価値ある情報の化体された有体物は財物とみなす」案	「有体物に化体された財産価値ある情報は財物とみなす」案	（１９８８年）刑法学会報告案	西ドイツ刑法 §２０２Ａ
客体となる情報	コンピュータ情報とマニュアル情報の区別			区別しない	区別しない	区別しない	区別しない	直接に知覚できない情報に限る（コンピュータ情報に限らない）
	情報の性質			媒体の財物性を判断する際、情報の財産価値を重視する場合と、しない場合がある	財産価値ある情報	財産価値ある情報	財産価値ある技術上または営業上の秘密情報（被害者にとっ財産価値のあることを要す）	性質の如何を問わない（行為者にたいして予定されていないもの）
		媒体への化体の要否		要	要	要	否	否
			伝送中の情報	対象外	対象外	対象外	対象となる	対象となる
	情報の管理態様			保有者が所持していること	保有者が所持していること	保有者が所持していること	秘密性の管理（セキュリティ措置、秘密保持契約等）	無権限アクセスに対するセキュリティ措置
行為態様	不正取得	媒体の移動の要否		要	要	否	否	否
		移動する場合	・媒体を一時持ち出しコピーする ・センター内で他人所有の媒体にコピーし持ち出す	可罰	可罰	可罰	可罰	可罰
		移動しない場合	・端末から呼出し、プリントアウト、またはコピーする	不可罰	不可罰	可罰	可罰	可罰
		媒体に化体して取得することの要否			要	要	否	否
			見読		不可罰	不可罰	可罰	可罰
	漏示	媒体の移動の要否		要	要	否	否	職務上知り得る情報の漏示は本罪の対象外（不正競争防止法で処罰）
		媒体に化体して漏示することの要否			要	要	否	
			口頭による漏示		不可罰	不可罰	可罰	
行為の目的				（不法領得）	（不法領得）	（不法領得）	窃用	目的の如何を問わない
その他				コピーに賦物性なし		コピーに賦物性あり	職務上知り得た情報の窃用も処罰される	本罪では、行為者に予定されていない情報を権限なく他人に取得させる行為が処罰される

〔コンピュータ情報の不正取得・漏示〕 犯罪類型の比較（アメリカ州法）

		アリゾナ州法（1978年） （その他13州同型）	フロリダ州法（1978年）	ネバダ州法（1983年）
	種　類			
客体となる情報	内　容	・「財産」（電子的データを含む情報，機械又は人に可読的なコンピュータ・ソフトウェア，プログラム、有形、無形を問わず価値あるものを含む） ・「サービス」（データ検索を含む）	・トレード・シークレット （①秘密で，②価値があり，③業務に使用され，④知らない者又は使用しない者よりも，業務に利益又は利益を得る機会を与えるもので，⑤セキュリティの講ぜられているもの） ・法により秘密とされたデータ，プログラム又はサポート・ドキュメンテーション	①無限定のデータ，フログラム，サポート・ドキュメント ②個人情報
	態　様		コンピュータ，コンピュータ・システム又はコンピュータ・ネットワークの内外に在るを問わない。	同　左
行為	不正取得	データ，プログラムを含む「財産」，又はデータ検索を含む「サービス」を取得する目的で，コンピュータ，コンピュータシステム又はコンピュータ・ネットワークに無権限でアクセスする行為が処罰される。 （不正取得未遂も処罰）	故意に，権限なく情報を取得することを処罰	上記①故意に，権限なく情報を取得すること，コピー，入力 上記②情報取得の目的で，故意に，権限なく，コンピューター，コンピュータ・システム又はコンピュータネットワークを使用すること。
	漏　示		情報の漏示を処罰	上記①漏示を処罰
限定要件		「偽罔」によるアクセス by means of false or fraudulent pretenses,representations or promises	上記トレード・シークレットについてはセキュリティ侵害	
その他		非財産的情報への無権限アクセスは第2級コンピュータ詐欺として処罰		使用も処罰される。

＊山口厚氏「アメリカにおけるコンピュータ・データの刑罰による保護」（刑法雑誌２８巻４号）より作成。

〔コンピュータ情報の不正取得・漏示〕 犯罪類型の比較（アメリカ州法）

		ヴァージニア州法（1984年）	コネティカット州法（1984年）	オクラホマ州法（1984年）
客体となる情報	種　類			
	内　容	①　コンピュータ詐欺 無形のデータ等を含む「財産」 ②　コンピュータ・トレスパス 無限定のデータ，プログラム，ソフトウエア ③　プライバシー侵害 個人の履用、給与，信用，金融等の情報 ④　コンピュータ・サービスの窃用	①コンピュータの窃用 データ記憶を含むサービス ②コンピュータ情報の不正使用 コンピュータ・システムに存する，通信される，又は作り出されるデータ ③コンピュータ・システムの使用に供されるデータ ④傍受 コンピュータ・システムの中のデータ	①無形の価値あるデータを含む「財産」 ②データ記憶を含むサービス
	態　様	②は通信されるものを含む	③はコンピュータ・システムの内外に在るを問わない	
行為	不正取得	上記①…「財産」詐取目的でコンピュータ又はネットワークを使用すること 上記②…一時的もしくは永続的に奪取し又はコピー作成の目的でコンピュータ又はネットワークを使用すること 上記③…検索すること 上記④…サービス取得の目的でコンピュータ又はネットワークを使用	上記①…サービス取得目的でのシステムへのアクセス 上記②…ディスプレイ，コピー 上記③…権限なき取得 上記④…傍受	①故意に，権限なく，コンピュータ，システム，ネットワークにアクセスしてコピー，取得すること ②サービスを詐取する目的で，コンピータ，システム，ネットワークを使用すること
	漏　示	上記①…横領の客体となる	上記②漏示処罰	①漏示処罰
限定要件				
その他			・不正取得されたデータを故意に収受又は保持すること ・不正に取得されたデータと知りつつ使用又は漏示すること 処罰	

犯罪類型の比較　(アメリカ州法)

[コンピュータ情報の不正取得・漏示]

		アラバマ州法 (1985年)	テキサス州法 (1985年)	ニューヨーク州法 (1986年)
客体となる情報	種　類			
	内　容	(知的財産の罪) データ，プログラム，サポート・ドキュメンテーション	①コンピュータに記憶又は保持されているデータ ②パスワード，識別コード，個人識別番号，その他コンピュータ・セキュリティ・システムに関する秘密情報	①コンピュータ・サービス (データのアウトプット，検索を含む) ②コンピュータ・トレスパス 次のデータ又は，プログラム ・個人の医療記録 ・政府の管理する個人情報 ・正当な占有者又はその同意によりアクセスが認められた者以外は利用できず，正当な占有者に，旗業者又はその他知識を有しない者よりも利益を与えるもの ③不法なコピー 無限定のデータ又はプログラム
	態　様	コンピュータ，システム，ネットワークの内外を問わない		
行為	不正取得	アクセス，通信，検索，取得を処罰	①故意に権限なくアクセスすること	①故意に，権限なくサービスを使用すること ②故意に，権限なくアクセスすること ③権限なくコピーすること
	漏　示	漏示処罰	②故意に，権限なく他人にあたえること	
限定要件			①セキュリティ・システムの存在を行為者が認識していること ②セキュリティ・システム設置者の有効な同意がないこと	①コンピュータ又はコンピュータ・システムの無権限使用を防止する機能を持つ装置又はコーディング・システムが設置又はプログラムされている場合に限る 無権限使用の警告（口頭，掲示，ディスプレイ等）も要する ②当該行為により故意に所有者から2.500ドル 以上の経済的価値を奪取又は取得する場合 重罪又はその未遂を犯す目的又はその遂行を推進する目的のある場合
その他		使用処罰 (形の加重) ・無形のデータを含む財産詐取の目的 ・知的財産の損害2500ドル以上の場合		不法に複写したコピーを，自己又は第三者の利益を図る目的で所持することを処罰

(3) 犯罪類型のあり方について —— 考え方の方向と問題点 ——

Ⅰ「前提となる問題意識」は、このテーマを検討するに当っての前提条件を述べたもので、当委員会においても、基本的にはほぼ共通の合意があるものと考えられる。

Ⅱの「犯罪類型のあり方」のうち、1.1「財産犯としての構成」については、63年度における委員会の討議で、種々の問題提起が行われたが、この方向への評価については意見が分れている。本稿は、これらの内容を事務局の理解を混えて、要約している。

Ⅱの1.2「秘密侵害犯、プライバシー侵害犯としての構成」及び2.「行為態様等を中心として犯罪類型を構成する方向」について、委員会では63年度に断片的ではあるが討議を行っているが、総合的には未検討である。今後検討を要する問題を、事務局の意見を混え摘記している。なお2は、システム侵害行為を基本として、①処罰範囲をさらに絞り込むためにどのような要件を必要とするか、及び②漏示をどのように扱うかを述べている。

I　前提となる問題意識

情報内容を不正にコピーし、あるいはプリントアウトして取得する行為は、情報の保有者による情報の利用可能性を奪わないという点で、使用窃盗に類似しているが、時として情報の保有者に重大な被害を及ぼす場合があるという点に特徴がある。

そのように情報の保有者に重大な被害を及ぼすような情報の不正取得や漏示を処罰するため、下級審判決は従来、情報を化体した媒体の一時持出しなど有体物の移動という外形面を捉えて窃盗、横領などの財物取得罪を適用してきた。

しかし①コンピュータ・システムによる情報化の進展に伴い、そのような方法によっては、対処し難い状況が現れている。即ち、コンピュータと通信の融合により、多くの重要な情報が企業等の内外の端末からアクセス可能となり、情報の大量化・多様化、検索の容易さ、処理の迅速性などと相俟って、媒体の移動を伴わずに情報の窃取等が行われる潜在的危険性が高まりつつある。これに対して、財物取得罪等現行刑法の規定を適用することは困難である。また②磁気テープなど情報の化体した媒体を一時社外に持ち出し不正にコピーするという事例についても、従来これに財物取得罪を適用してきた裁判所の解釈は、情報の使用窃盗的性質に起因する不法領得概念の拡大適用という、些か強引な操作に基づいて行われてきた嫌いがある。この点について、情報化の進展を正視して、今後の適切な方向を検討する必要がある。さらに③国際通信網の拡大により、情報の国際的交流が活発化しつつあるが、その円滑な展開を図るには、情報の保護について適切な対策を必要とするものと考えられ、諸外国においてはそのような観点を含めて立法措置が進められている。

以上の理由に基づき、情報の不正取得・漏示に関し、立法的対応を検討すべき状況にあると判断されるが、検討に当たっては次の点が前提になるものと考えられる。

即ち、企業や個人の日常の活動は情報の利用、収集、提供に基づいて行われて

いる。情報の中の或るものは、媒体に化体して保有者の所持管理下におかれるが、そのような情報の利用、収集、提供は必ずしも常に正当な権限に基づいて行われるとは限らない。しかしその多くは、有体物の使用窃盗が不可罰とされる以上に、当罰性は少ないものと思われる。当罰性が問題となるのは、情報の無権限の取得や漏示の中の著しく不当な或る特定のケースであると考えられる。立法化に当たっては、当罰性が問題なく肯定できるようなケースに特定して犯罪化するという配慮が必要である。

以上の事情は、構成要件の定め方次第によっては、直ちに過剰処罰の問題が浮上することを意味する。そのことは、かつて刑法改正草案の企業秘密漏示罪に関して、企業秘密の概念の不明瞭性と、これによる過剰処罰の危険が問題として指摘され、さらに公共目的による内部告発や公害調査の抑圧、国家機密保護罪への波及等が憂慮されて、提案が凍結に導かれた経緯からも明らかであろう。

II 犯罪類型のあり方

1. 客体となる情報の性質を中心として犯罪類型を構成する方向

1.1 財産犯としての構成

1）財産犯としての構成は、趣旨がわかりやすく、肯定できる側面を持っている。すなわち、

① 企業には、無体財産権で保護される情報のほかにも、多年の努力と費用を投入して得た財産価値ある情報が少なくない（例えば特許申請中ないしは手続きや要件等の関係で特許出願をしない情報、著作権の要件をみたさない顧客情報など）。

これらの情報がコピーされて競争相手企業の手に渡れば、保有者の情報に対する独占的利用の地位は崩れ、情報の財産価値は一挙に失われる。それは、行為自体が極めて不当であるだけでなく、企業が新しい技術や営業方法を企画、開発する意欲を失わせるという意味で社会経済的にも大きな弊害をもたらすこととなる。

このような典型的事例の当罰性については是認できる余地が多いと考えられる。

② また、財産犯として捉える方向自体は、伝統的な刑法の枠組みになじみやすいといえる。

判例においても、(a)情報が化体された媒体の財物性は、情報の切り離された媒体の素材だけについてではなく、情報と媒体が合体したものの全体について判断すべきであるとされ（新薬産業スパイ事件）、(b)媒体を一時社外へ持ち出し、化体された情報を不正にコピーした事例について、窃盗、横領罪が適用されている（建設調査会事件、上記新薬産業スパイ事件、新潟鉄工所事件）。その構成に、不法領得概念の拡大解釈の問題は残るとしても、当罰性自体については殆ど異論がないようである。

2）しかし財産犯として構成する方向は、以上のように肯定的な側面を持つ反面、“財産価値ある情報”という概念が明確さを欠くため、規定の解釈運用のいかんによっては処罰範囲が過剰に広がる危険性を含んでいる。

その理由は、(a)情報の財産的価値は開発、購入、収集などのコスト（取得価額）だけでなく、情報の利用によって、形成される場合があること、(b)コンピュータ・システムの進展により情報の多角的利用が飛躍的に増大しつつあることに基づいている。

すなわち従来財産価値があるとは考えられなかった情報に、新たな利用目的が考案されて価値を生ずるというケースは少なくない。情報が不正に取得される場合は、その情報が正常な手続きで提供されたとすれば得られたであろう潜在的な価値の喪失を意味する場合がある。このように新たな利用に伴う潜在的価値の観点を入れれば、財産価値ある情報の範囲は著しく拡大するであろう。

また、財産価値ある情報が不正取得されれば、不正取得者当人に使用

目的がなくとも、流通によってライバル企業の手に渡って価値を失ったり、あるいは新たな利用による潜在的価値を得る機会を失うことになる。そのような財産価値の潜在的損失という観点を入れるならば、財産的価値の範囲は一層広がることとなろう。

財産犯の類型として、従来の財物取得罪を類推し（判例）、あるいは財物概念の微調整によって手当てする（イギリス方式）という方向は、伝統的な財物取得罪からの飛躍を避けるという意味では慎重な姿勢であると考えられる。しかし前記のように情報の財産価値が利用によって大きく左右されるという特性を持ち、しかも、コンピュータ・システムによって処理される情報の量や利用可能性が急激に増加している事実を併せ考えるならば、処罰範囲の過剰な拡大という危険を免れないと思われる。

（注）

１９８８年の“刑法学会報告案”は、処罰範囲を被害者にとって財産価値のある技術上または営業上の秘密情報が窃用の目的で不正取得または漏示される場合に限定することによって、情報犯罪の肥大化を抑制しようと試みている。これは、その意図において意義あるものと考えられるが、(a)国家機密への波及を避け得るか否か、(b)後述のように特に漏示について過剰処罰の問題を生じないか、(c)逆に当罰性のある行為－例えば重大な業務妨害の結果を生ずる場合が処罰範囲から洩れるのではないか、といった問題があり得るであろう。

3）以上のように財産犯として構成する方向は、客体となる財産的情報の概念が不明瞭であるという問題を含むのであって、この点について当委員会としては、委員によりニュアンスの差はあるにしても、ほぼ共通の認識があるものと思われる。

唯、財産犯として構成する方向への評価については、委員会内部でも

意見が分かれている。大きく分けると次の三つの意見がある。

① どのような被害から、刑法的な保護を必要とするかという観点からみると、当罰的な行為とは、結局財産的被害の大きい不正行為である。とりわけそのような不正行為の処罰が媒体の移動によって左右されているという現実の矛盾が立法措置を緊要とする主たる原因である。

財産的情報の概念自体は不明瞭であるにしても、行為態様等を明確化することによって、より具体的な形で犯罪類型を規定することは可能であり、そのような方向を選択することが最も現実的で弊害も少ないと考えられる。

② コンピュータのデータやプログラムは、収集・開発コストによって価値が作られるほか、利用者によって新たに価値が生み出され、それに応じて交換価値も変わる。そのような状況は有体物についてもある程度言えるが、コンピュータ情報については、著しくその傾向が強い。

コンピュータ情報について効用価値を考慮に入れると、「財産価値を有する情報」という構成要件は、あいまい過ぎて意味を為さない。

したがって財産犯という捉え方自体に無理があるとみるべきであり、角度を変えてシステム侵害行為を中心とした行為態様等の面から犯罪類型を考える必要がある。

③ 一つの犯罪類型で当罰的行為のすべてをカヴァーすることには無理がある。情報の財産価値を保護するという観点から、財産価値の明確な情報を客体とする不正行為を財産犯として捉えるとともに、それ以外の情報を客体とする不正行為を、個人プライバシーの保護や、コンピュータ・システムに関係する経済利益の保護という観点から捉える犯罪類型をそれぞれ別に考える必要がある。

なお、犯罪類型を構成する方向の相違は、立法の形式に影響することとなる。即ち、財産犯として構成する類型は刑法になじみやすいが、個

人のプライバシーやコンピュータ・システムを保護するための犯罪類型は、行政刑法のような特別法に規定することとなろう。但し、①刑法に規定する場合は、自然的な反倫理行為から構成されている刑法の中に、コンピュータ情報その他情報を刑罰による保護の対象とする新しい犯罪類型を入れることについて従来から強い反対があるので実現に少なからず困難があること、他方②行政刑法に規定する場合は、短期の懲役または罰金が課されることとなるが、日本では通常、略式命令による軽い罰金で処理される例が多く、予防効果に疑問のあることが問題として指摘されている。

以上のように財産犯として捉える方向については意見が分かれているが、いずれにしても、今後の課題として財産的情報以外の情報をどのように扱うか、また行為様態等の面から、どのような犯罪類型を考え得るかを、さらに検討する必要がある。そのために想定される事実について当罰性の検証をさらに綿密に行うことが必要視される。

1.2 秘密侵害犯（プライバシー侵害犯）としての構成

1）上記のように財産的情報の概念は、不明確で広がりを持つ可能性があるが、それに含まれない情報もあり得る。

企業の経営情報については、債権者の保護や公正な投資機会の確保を図るという見地から、ある程度の開示が必要とされ、一定範囲で法的義務も課されているが、一方経営情報の中には、事業計画や製品企画の初期段階のデータのように、計画を円滑に実施する上で外部に知られたくない情報があり、また企業はいずれも何らかの問題を抱えており、これが外部へ洩れると企業の信用やイメージの失墜につながる場合も少なくない。

これらは財産的情報として捉え難い場合があり、そのような情報を保護するためには、秘密侵害犯として犯罪類型を構成する方向が考えられる。

“秘密情報”の範囲については、セキュリティ措置のような形式要件で捉える方法（西ドイツ刑法§２０２Ａ）と、実質秘で捉える方法が考えられるが、前者の場合情報の範囲は無制限であり、後者の場合も“秘密性”と“財産価値”は相互に依存し合う関係となるため情報の範囲の限定としては不明確で、過剰処罰の問題を免れないと思われる。

したがって、企業の経営情報等に対する不正取得が当罰性を持つ場合があるとすれば、行為様態等における積極的な不正が要件として必要視される。

２）次に企業が保有する個人情報については、例えば個人の商品購入歴、クレジットの返済歴のように、特定の個人のプライバシーに係わる情報がダイレクト・マーケティングやクレジットの利用促進のために営業情報として使用され、これらの個人情報のファイルは、企業の重要な財産的秘密情報として取扱われる。このように同一の個人情報が利用の目的や態様によって異る様相を呈することとなるが、個人情報の特色として注意すべき点は、個人情報が企業財産として管理されている場合にも、個人情報の収集、利用に関しては、基本的には、情報主体である個人のコントロールに服すべきであるということである。したがって個人情報の不正取得等は、このような情報主体による自己情報のコントロールに対する侵害という性格を持っている。

個人情報の刑法的保護を、情報主体の保護という観点からとりあげることについては、①特に民間部門については、政策的に企業等の自主規制と立法化のいずれを選択すべきかという問題があり、また②立法化に当たっても、情報主体による自己情報のコントロールの原理を中心とする規律を考える必要があること等の事情から、企業情報とは別個に検討することが適切であろう。

2. 行為様態等を中心として犯罪類型を構成する方向

以上のように客体である情報の性質・内容からのアプローチによる場合は、困難な問題が少なくない。

したがって行為態様等の面からのアプローチが同時に必要視される。これについては次の点に特に留意すべきであろう。

1）財物の領得は、保有者の利用可能性を奪うことを本質とし、行為態様としては保有者の所持管理下にある財物を取ることで足りる。これに反し情報の不正取得は、保有者の利用可能性を残らず奪うのではなく、その独占的な利用可能性を奪うことに特色がある。保有者の情報に対する独占的な利用可能性は、情報の化体した媒体を所持管理すること（建物の中におく等）のみによって確保されず、不正アクセスに対するセキュリティ対策（オンライン情報に対するアクセス・コントロールやオフライン情報の化体した媒体の保管・受渡し管理等）によってはじめて確保し得るものである。

したがって情報の不正取得についての当罰性は、単に権限なくコンピュータ・システムに侵入したことによってではなく、その情報に対するセキュリティ対策の侵害によって生ずると考えるのが適切なのではないか。

2）情報の不正取得は、セキュリティ対策の侵害を要件とすることによって処罰範囲が限定されるが、企業のセキュリティ対策は情報内容のいかんに係わらず、企業の主観的意図によって行われる。そのような企業の主観性によって処罰範囲が左右されることを避けるとともに、処罰範囲をさらに限定するために、行為の目的（利得、加害等）、行為の客体（情報の財産的価値等）、あるいは行為の結果（財産的損害、業務妨害等）を、必要に応じ複数を組み合せて要件とすることが考えられる。

3）不正取得の態様として、取得した情報を媒体に固定することを要件とすべきかという点は、一般的には肯定されるが、試験問題の入手や、株

式、不動産などの投機売買に利用するための経営情報の入手等については、記憶可能な一片の情報によって目的が達せられることも考慮する必要がある。

4）情報の漏示については、次のように考えられる。

財産的情報や秘密情報を保護する観点から立法される場合は当然、不正取得と並んで漏示も処罰される。コンピュータ・システムを保護する観点から立法される場合は、不正アクセスないし情報の不正取得が処罰されることと並んで、漏示も処罰するか否かは立法政策上の選択となるようであるが、処罰される場合が多い（アメリカの州法）。

日本の場合、漏示については、次の理由により慎重に扱うことが必要と考えられる。

① コンピュータ・システムの進展に伴い、情報の多角的利用が企業間提携と相俟って増加しており、情報の提供、交換や取材協力は、日常的に頻繁に行われている一方で契約等による守秘義務の慣行は未だ定着していない状況である。

② 日常的に頻繁に行われている情報の提供・交換などの中から、特定の当罰的行為を的確に抑える必要があるとすれば、犯罪捜査活動等による波及的なインパクトを最小限にとどめるという意味でも、限定的で明確なメルクマールが必要である。

特定の職業、身分、地位に在る者に対し、いくつかの個別立法によって守秘義務を課し、違反行為を処罰することとしているのは、そのような方向の現れとみられる。

そのほか、より一般的な形では、前記“刑法学会報告案”が、客体となる情報及び行為の目的を“被害者にとって財産価値ある技術上又は営業上の秘密情報を窃用の目的で”という要件で限定した上で、漏示を犯罪としているのが、その一つの試みである。しかしこの案によれば、従業員等の転職や独立に際しての情報の持ち出しが、契約によ

る守秘義務違反を条件として広く処罰対象に包含され、口頭による漏示も処罰され得るという点で、過剰処罰の問題を避けられないのではないかと思われる。

③ 従業員等の転職や分離・独立の場合は、少なくともその従業員が在職中に自ら開発し、又はリヴァース・エンジニアリングによって得た情報については、転職の自由、技術開発促進の見地から、刑事責任を問わないほか、契約による民事的な拘束も最小限にとどめる配慮が必要ではないかと考えられる。

その他の場合も、情報の持ち出しを制限することが必要であるとすれば原則的には民事契約により、退職後は合理的な期間内に限定して守秘義務で拘束するのが妥当であろう。

唯、他の従業員等が開発した価値ある情報を、情報を管理する者等が利得や競業の目的で漏示し、企業に致命的な損害を与える等のケースについては、守秘義務違反だけでなく、業務妨害等の客観的な要素をメルクマールとして当罰性を考える余地があろう。

3. 以上のいずれの方向で犯罪類型を検討する際にも、国家機密保護罪への波及や、公共目的による内部告発、公害調査の抑圧等の問題を避けるための配慮が必要であろう。

そのような観点から例えば個人のプライバシーや企業等の業務遂行（営業の自由）を保護するため、情報の不正取得による個人のプライバシー侵害や企業の業務妨害を中心に犯罪類型を構成する方向も考えられる。この方向を選択する場合は国家秘密保護の問題はおのずから検討対象から除外されるとともに、経営情報の秘匿を含む営業活動の自由は、公共的利益のために制限されることを前提として、刑法的保護を考慮することとなろう。

参考資料

参考資料

1. 関係法令

1 刑 法

第２３５条【窃盗】

他人ノ財物ヲ窃取シタル者ハ窃盗ノ罪ト為シ１０年以下ノ懲役ニ処ス

第２４６条【詐欺】

① 人ヲ欺罔シテ財物ヲ騙取シタル者ハ１０年以下ノ懲役ニ処ス

② 前項ノ方法ヲ以テ財産上不法ノ利益ヲ得又ハ他人ヲシテ之ヲ得セシメタル者亦同シ

第２４７条【背任】

他人ノ為メ其事務ヲ処理スル者自己若クハ第三者ノ利益ヲ図リ又ハ本人ニ損害ヲ加フル目的ヲ以テ其任務ニ背キタル行為ヲ為シ本人ニ財産上ノ損害ヲ加ヘタルトキハ５年以下ノ懲役又ハ千円以下ノ罰金ニ処ス

第２５２条【横領】

① 自己ノ占有スル他人ノ物ヲ横領シタル者ハ５年以下ノ懲役ニ処ス

② 自己ノ物ト雖モ公務所ヨリ保管ヲ命セラレタル場合ニ於テ之ヲ横領シタル者亦同シ

第２５３条【業務上横領】

業務上自己ノ占有スル他人ノ物ヲ横領シタル者ハ１０年以下の懲役ニ処ス

第２５６条【贓物収受、故買等】

① 贓物ヲ収受シタル者ハ３年以下ノ懲役ニ処ス

② 贓物ノ運搬、寄蔵、故買又ハ牙保ヲ為シタル者ハ10年以下ノ懲役及ヒ千円以下ノ罰金ニ処ス

第１３章　秘密ヲ侵ス罪

第１３３条【信書開披】

故ナク封緘シタル信書ヲ開披シタル者ハ１年以下ノ懲役又ハ２百円以下ノ罰金ニ処ス

第１３４条【秘密漏泄】

①　医師、薬剤師、薬種商、産婆、弁護士、弁護人、公証人又ハ此等ノ職ニ在リシ者故ナク其業務上取扱ヒタルコトニ付キ知得タル人ノ秘密ヲ漏泄シタルトキハ６月以下ノ懲役又ハ百円以下ノ罰金ニ処ス

②　宗教若クハ禱祀ノ職ニ在ル者又ハ此等ノ職ニ在リシ者故ナク其業務上取扱ヒタルコトニ付キ知得タル人ノ秘密ヲ漏泄シタルトキ亦同シ

第１３５条【親告罪】

本章ノ罪ハ告訴ヲ待テ之ヲ論ス

2　憲　法

第２１条【集会・結社・表現の自由、通信の秘密】

①　集会、結社及び言論、出版その他一切の表現の自由は、これを保障する。

②　検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。

第３３条【逮捕の要件】

何人も、現行犯として逮捕される場合を除いては、権限を有する司法官憲が発し、且つ理由となつてゐる犯罪を明示する令状によらなければ、逮捕されない。

第３５条【住居の不可侵】

①　何人も、その住居、書類及び所持品について、侵入、捜索及び押収を受けることのない権利は、第３３条の場合を除いては、正当な理由に基いて発せられ、且つ捜索する場所及び押収する物を明示する令状

がなければ、侵されない。

② 捜索又は押収は、権限を有する司法官憲が発する各別の令状により、これを行ふ。

3 郵便法

第8条（検閲の禁止）

郵便物の検閲は、これをしてはならない。

第9条（秘密の確保）

① 郵政省の取扱中に係る信書の秘密は、これを侵してはならない。

② 郵便の業務に従事する者は、在職中郵便物に関して知り得た他人の秘密を守らなければならない。その職を退いた後においても、同様とする。

第80条（信書の秘密を侵す罪）

① 郵政省の取扱中に係る信書の秘密を侵した者は、これを1年以下の懲役又は2万円以下の罰金に処する。

② 郵便の業務に従事する者が前項の行為をしたときは、これを2年以下の懲役又は5万円以下の罰金に処する。

第85条（未遂罪及び予備罪）

① 第76条乃至第78条、第80条、第83条及び前条の未遂罪は、これを罰する。

② 前条の罪を犯す目的でその予備をした者は、これを2年以下の懲役又は1万円以下の罰金に処し、その用に供した物は、これを没収する。

4 電気通信事業法

（検閲の禁止）

第3条

電気通信事業者の取扱中に係る通信は、検閲してはならない。

（秘密の保護）

第４条

① 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。

② 電気通信事業に従事する者は、在職中電気通信事業者の取扱中に係る通信に関して知り得た他人の秘密を守らなければならない。その職を退いた後においても、同様とする。

（適用除外等）

第９０条

① この法律の規定は、次に掲げる電気通信事業については、適用しない。

一 専ら一の者（電気通信事業者たる一の者を除く。）に電気通信役務を提供する電気通信事業

二 その一の部分の設置の場所が他の部分の設置の場所と同一の構内（これに準ずる区域内を含む。）又は同一の建物内である電気通信設備その他郵政省令で定める基準に満たない規模の電気通信設備により電気通信役務を提供する電気通信事業

三 電気通信設備を用いて他人の通信を媒介する電気通信役務以外の電気通信役務を提供する第二種電気通信事業

② 前項の規定にかかわらず、第３条及び第４条の規定は、同項各号に掲げる電気通信事業を営む者の取扱中に係る通信についても適用する。

第１０４条

① 電気通信事業者の取扱中に係る通信（第９０条第２項に規定する通信を含む。）の秘密を侵した者は、１年以下の懲役又は３０万円以下の罰金に処する。

② 電気通信事業に従事する者が前項の行為をしたときは、２年以下の懲役又は５０万円以下の罰金に処する。

③ 前２項の未遂罪は、罰する。

5　有線電気通信法

（有線電気通信の秘密の保護）

第９条

有線電気通信（電気通信事業法第４条第１項又は第９０条第２項の通信たるものを除く。）の秘密は、侵してはならない。

第１４条

① 第９条の規定に違反して有線電気通信の秘密を侵した者は、１年以下の懲役又は２０万円以下の罰金に処する。

② 有線電気通信の業務に従事する者が前項の行為をしたときは、２年以下の懲役又は３０万円以下の罰金に処する。

第１５条

前２条の未遂罪は、罰する。

6　電波法

（秘密の保護）

第５９条

何人も法律に別段の定めがある場合を除くほか、特定の相手方に対して行われる無線通信（電気通信事業法第４条第１項又は第９０条第２項の通信たるものを除く。第１０９条において同じ。）を傍受してその存在若しくは内容を漏らし、又はこれを窃用してはならない。

第１０９条

① 無線局の取扱中に係る無線通信の秘密を漏らし、又は窃用した者は、１年以下の懲役又は２０万円以下の罰金に処する。

② 無線通信の業務に従事する者がその業務に関し知り得た前項の秘密を漏らし、又は窃用したときは、２年以下の懲役又は３０万円以下の罰金に処する。

7　著作権法

（著作物の例示）

第１０条

この法律にいう著作物を例示すると、おおむね次のとおりである。

九　プログラムの著作物

3　第１項第９号に掲げる著作物に対するこの法律による保護は、その著作物を作成するために用いるプログラム言語、規約及び解法に及ばない。この場合において、これらの用語の意義は、次の各号に定めるところによる。

一　プログラム言語　プログラムを表現する手段としての文字その他の記号及びその体系をいう。

二　規　約　特定のプログラムにおける前号のプログラム言語の用法についての特別の約束をいう。

三　解　法　プログラムにおける電子計算機に対する指令の組合せの方法いう。

（データベースの著作物）

第１２条の２

データベースでその情報の選択又は体系的な構成によって創作性を有するものは、著作物として保護する。

2　前項の規定は、同項のデータベースの部分を構成する著作物の著作者の権利に影響を及ぼさない。

第１１９条

次の各号のいずれかに該当する者は、３年以下の懲役又は百万円以下の罰金に処する。

一　著作者人格権、著作権、出版権又は著作隣接権を侵害した者（第３０条（第１０２条第１項において準用する場合を含む。）に定める私的使用の目的をもつて自ら著作物又は実演等の複製を行つた者

を除く。）

二　営利を目的として、第３０条に規定する自動複製機器を著作権、出版権又は著作隣接権の侵害となる著作物又は実演等の複製に使用させた者

8　国家公務員法

（秘密を守る業務）

第１００条

①　職員は、職務上知ることのできた秘密を漏らしてはならない。その職を退いた後といえども同様とする。

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

③　前項の許可は、法律又は政令の定める条件及び手続に係る場合を除いては、これを拒むことができない。（昭和４０法６９本項改正）

④　前３項の規定は、人事院で扱われる調査又は審理の際人事院から求められる情報に関しては、これを適用しない。何人も、人事院の権限によつて行われる調査又は審理に際して、秘密の又は公表を制限された情報を陳述し又は証言することを人事院から求められた場合には、何人からも許可を受ける必要がない。人事院が正式に要求した情報について、人事院に対して、陳述及び証言を行わなかつた者は、この法律の罰則の適用を受けなければならない。（昭和２３法２２２本項追加）

第１０９条

左の各号の一に該当する者は、１年以下の懲役又は３万円以下の罰金に処する。

十二　第１００条第１項又は第２項の規定に違反して秘密を漏らした者

9　地方公務員法

（秘密を守る義務）

第３４条

①　職員は、職務上知り得た秘密を漏らしてはならない。その職を退いた後も、また、同様とする。

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

③　前項の許可は、法律に特定の定がある場合を除く外、拒むことができない。

（罰則）

第６０条

左の各号の一に該当する者は、１年以下の懲役又は３万円以下の罰金に処る。

二　第３４条第１項又は第２項の規定（第９条第１２項において準用する場合を含む。）に違反して秘密を漏らした者

１０　所得税法

第２４３条

所得税に関する調査に関する事務に従事している者又は従事していた者が、その事務に関して知ることのできた秘密を漏らし又は盗用したときは、これを２年以下の懲役又は３万円以下の罰金に処する。

１１　法人税法

第１６３条

法人税の調査に関する事務に従事している者又は従事していた者が、その事務に関して知ることのできた秘密を漏らし又は盗用したときは、これを２年以下の懲役又は３万円以下の罰金に処する。

１２　自衛隊法

（秘密を守る義務）

第５９条

① 隊員は、職務上知ることのできた秘密を漏らしてはならない。その職を離れた後も、同様とする。

② 隊員が法令による証人、鑑定人等となり、職務上の秘密に属する事項を発表する場合には、長官の許可を受けなければならない。その職を離れた後も、同様とする。

③ 前項の許可は、法令に別段の定がある場合を除き、拒むことができない。

第１１８条

① 次の各号の一に該当する者は、１年以下の懲役又は３万円以下の罰金に処する。

一　第５９条第１項又は第２項の規定に反して秘密を漏らした者

１３　特許法

（秘密を漏らした罪）

第２００条

特許庁の職員又はその職にあつた者がその職務に関して知得した特許出願中の発明に関する秘密を漏らし、又は盗用したときは、１年以下の懲役又は５万円以下の罰金に処する。

１４　実用新案法

（秘密を漏らした罪）

第６０条

特許庁の職員又はその職にあつた者がその職務に関し知得した実用新案登録出願中の考案に関する秘密を漏らし、又は盗用したときは、１年以下の懲役又は５万円以下の罰金に処する。

１５　意匠法

（秘密を漏らした罪）

第７３条

特許庁の職員又はその職にあつた者がその職務に関して知得した意匠登録出願中の意匠に関する秘密を漏らし、又は盗用したときは、１年以下の懲役又は５万円以下の罰金に処する。

１６　私的独占の禁止及び公正取引の確保に関する法律

第３９条【委員・職員等の秘密保持義務】

委員長、委員及び公正取引委員会の職員並びに委員長、委員又は公正取引委員会の職員であつた者は、その職務に関して知得した事業者の秘密を他に漏し、又は窃用してはならない。

第９３条【秘密保持義務違反の罪】

第３９条の規定に違反した者は、これを１年以下の懲役又は１０万円以下の罰金に処する。

１７　公認会計士法

（秘密を守る義務）

第２７条

公認会計士又は会計士補は、正当な理由がなく、その業務上取り扱つ

たことについて知り得た秘密を他に漏らし、又は窃用してはならない。公認会計士又は会計士補でなくなつた後であつても同様とする。

第５２条

① 第２７条（第１６条の２第４項において準用する場合を含む。）又は第４９条の２の規定に違反した者は、２年以下の懲役又は３万円以下の罰金に処する。

② 前項の罪は、告訴を待つて、これを論ずる。

１８ 証券取引法

第１０６条【役職員の秘密保持義務】

証券取引所の役員若しくは職員又はこれらの職にあつた者は、その職務に関して知得した秘密を他に漏らし、又は窃用してはならない。

第１５６条の１１【役職員の秘密保持義務】

第１０６条の規定は、証券金融会社の役員若しくは職員又はこれらの職にあつた者について準用する。

第２０４条【秘密を漏らす罪】

第１０６条（第１５６条の１１において準用する場合を含む。）の規定に違反した者は、これを１年以下の懲役又は１０万円以下の罰金に処する。

１９ 商品取引所法

（取引所の役員及び使用人等の秘密保持義務）

第１４４条

取引所の役員若しくは使用人又はこれらの職にあつた者は、取引所の役員又は使用人としてその職務に関して知得した秘密を他に漏らし、又はせつ用してはならない。

第１５８条

第１４４条の規定に違反した者は、１年以下の懲役又は１０万円以下の罰金に処する。

２０　行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律

第１３条

３　保有機関の長は、開示請求があつたときは、次条第１項に掲げる場合を除き、開示請求をした者（以下「開示請求者」という。）に対し、書面により、当該開示請求に係る処理情報について開示をしなければならない。ただし、開示請求者の同意があるときは、書面以外の方法により開示をすることができる。

第２５条

偽りその他不正の手段により、第１３条第３項の規定による開示を受けた者は、１０万円以下の過料に処する。

２１　日米相互防衛援助協定等に伴う秘密保護法

（定義）

第１条

①　この法律において「日米相互防衛援助協定等」とは、日本国とアメリカ合衆国との間の相互防衛援助協定、日本国とアメリカ合衆国との間の船舶賃借協定及び日本国に対する合衆国艦艇の貸与に関する協定をいう。

②　この法律において「装備品等」とは、船舶、航空機、武器、弾薬その他の装備品及び資材をいう。

③　この法律において「防衛秘密」とは、左に掲げる事項及びこれらの事項に係る文書、図面又は物件で、公になつていないものをいう。

一　日米相互防衛援助協定等に基き、アメリカ合衆国政府から供与された装備品等について左に掲げる事項

イ　構造又は性能

ロ　製作、保管又は修理に関する技術

ハ　使用の方法

ニ　品目及び数量

二　日米相互防衛援助協定に基き、アメリカ合衆国政府から供与された情報で、装備品等に関する前号イからハまでに掲げる事項に関するもの

（防衛秘密保護上の措置）

第２条

防衛秘密を取り扱う国の行政機関の長は、政令で定めるところにより、防衛秘密について、標記を附し、関係者に通知する等防衛秘密の保護上必要な措置を講ずるものとする。

（罰則）

第３条

①　左の各号の一に該当する者は、１０年以下の懲役に処する。

一　わが国の安全を害すべき用途に供する目的をもつて、又は不当な方法で、防衛秘密を探知し、又は収集した者

二　わが国の安全を害する目的をもつて、防衛秘密を他人に漏らした者

三　防衛秘密を取り扱うことを業務とする者で、その業務により知得し、又は領有した防衛秘密を他人に漏らしたもの

②　前項第２号又は第３号に該当する者を除き、防衛秘密を他人に漏らした者は、５年以下の懲役に処する。

③　前２項の未遂罪は、罰する。

第４条

① 防衛秘密を取り扱うことを業務とする者で、その業務により知得し、又は領有した防衛秘密を過失により他人に漏らしたものは、２年以下の禁こ又は５万円以下の罰金に処する。

② 前項に掲げる者を除き、業務により知得し、又は領有した防衛秘密を過失により他人に漏らした者は、１年以下の禁こ又は３万円以下の罰金に処する。

第５条

① 第３条第１項の罪の陰謀をした者は、５年以下の懲役に処する。

② 第３条第２項の罪の陰謀をした者は、３年以下の懲役に処する。

③ 第３条第１項の罪を犯すことを教唆し、又はせん動した者は、第１項と同様とし、同条第２項の罪を犯すことを教唆し、又はせん動した者は前項と同様とする。

④ 前項の規定は、教唆された者が教唆に係る犯罪を実行した場合において、刑法（明治４０年法律第４５号）総則に定める教唆の規定の適用を排除するものではない。

（自首減免）

第６条

第３条第１項第１号若しくは第３項又は前条第１項若しくは第２項の罪を犯した者が自首したときは、その刑を減軽し、又は免除する。

（この法律の解釈適用）

第７条

この法律の適用にあたつては、これを拡張して解釈して、国民の基本的人権を不当に侵害するようなことがあつてはならない。

22　日本国とアメリカ合衆国との間の相互協力及び安全保障条約第6条に基づく施設及び区域並びに日本国における合衆国軍隊の地位に関する協定の実施に伴う刑事特別法

（合衆国軍隊の機密を侵す罪）

第6条

① 合衆国軍隊の機密（合衆国軍隊についての別表に掲げる事項及びこれらの事項に係る文書、図画若しくは物件で、公になつていないものをいう。以下同じ。）を、合衆国軍隊の安全を害すべき用途に供する目的をもつて、又は不当な方法で、探知し、又は収集した者は、10年以下の懲役に処する。

② 合衆国軍隊の機密で、通常不当な方法によらなければ探知し、又は収集することができないようなものを他人に漏らした者も、前項と同様とする。

③ 前2項の未遂罪は、罰する。

第7条

① 前条第1項又は第2項の罪の陰謀をした者は、5年以下の懲役に処する。

② 前条第1項又は第2項の罪を犯すことを教唆し、又はせん動した者も、前項と同様とする。

③ 前項の規定は、教唆された者が、教唆に係る犯罪を実行した場合において、刑法総則に定める教唆の規定の適用を排除するものではない。

第8条

第6条第1項の罪、同項に係る同条第3項の罪又は同条第1項に係る前条第1項の罪を犯した者が自首したときは、その刑を減軽し、又は免除する。

② 全項の罪を犯した者が、証言した事件の裁判の確定前に自白したときは、その刑を減軽し、又は免除することができる。

③　合衆国軍事裁判所の手続に従って宣誓した鑑定人又は通訳人が虚偽の鑑定又は通訳をしたときは、前2項の例による。

（軍用物を損壊する等の罪）

第5条

合衆国軍隊に属し、且つ、その軍用に供する兵器、爆弾、糧食、被服その他の物を損壊し、又は傷害した者は、5年以下の懲役又は5万円以下の罰金に処する。

国家秘密法案新旧条文対照表

（注1）一九八五年六月自民党より国会に提出、同年十二月廃案

（注2）一九八六年五月自民党内で作成

修正案（注1）	旧法案（注2）
防衛秘密に係るスパイ行為等の防止に関する法律案	国家秘密に係るスパイ行為等の防止に関する法律案
（目的） 第一条　この法律は、防衛秘密の保護に関する措置を定めるとともに、外国に通報する目的をもって防衛秘密を探知し、若しくは収集し、又は防衛秘密を外国に通報する行為を処罰することにより、これらのスパイ行為等を防止し、もって我が国の安全に資することを目的とする。	（目的） 第一条　この法律は、外国のために国家秘密を探知し、又は収集し、これを外国に通報する等のスパイ行為等を防止することにより、我が国の安全に資することを目的とする。
（定義） 第二条　この法律において「防衛秘密」とは、「防衛及び外交に関する別表に掲げる事項並びにこれらの事項に係る文書、図画又は物件で、我が国の防衛上秘匿することを要し、かつ、公になっていないものをいう。 2　この法律において「不当な方法」とは、法令に違反し、対価を供与し、偽計を用い、又は、秘匿状態にある文書、図画等をみだりに開披する等社会通念上是認することのできない方法をいう。	（定義） 第二条　この法律において「国家秘密」とは、防衛及び外交に関する別表に掲げる事項並びにこれらの事項に係る文書、図画又は物件で、我が国の防衛上秘匿することを要し、かつ、公になっていないものをいう。
（防衛秘密保護上の措置） 第三条　国の行政機関の長は、その取り扱う防衛秘密に属する事項又は文書、図画若しくは物件を防衛秘密として指定しなければならない。ただし、その指定に当たっては、いやしくも防衛秘密に属しないものを指定するようなことがあってはならない。 2　国の行政機関の長は、前項の規定により防衛秘密として指定した事項は文書、図画若しくは物件について常に点検を行い、我が国の防衛上秘匿する必要がなくなったとき、又は公になったものがあるときは、速やかに、その指定を解除しなければならない。 3　国の行政機関の長は、政令で定めるところにより、防衛秘密について、取扱責任者及び取扱者を定め、標記を付し、関係者に通知する等防衛秘密の保護上必要な措置を講じなければならない。	4　前項の措置を講ずるに当たり、国の行政機関の長は、防衛秘密を国の行政機関以外の者に取り扱わせる場合には、これを取り扱う者に対し防衛秘密であることを周知させるための特別な配慮をしなければならない。 5　防衛秘密を取り扱う者は、これが漏れることのないよう最大の注意をしなければならない。
（国家秘密保護上の措置） 第三条　国家秘密を取り扱う国の行政機関の長は、政令で定めるところにより、国家秘密等国家秘密の保護上必要な措置を講ずるものとする。	2　前項の措置を講ずるに当たり、国家秘密を取り扱う国の行政機関の長は、国家秘密を国の行政機関以外の者に取り扱わせる場合には、これを取り扱う者に対し国家秘密であることを周知させるための特別な配慮をしなければならない。
（罰則） 第四条　次の各号の一に該当する者は、無期又は三年以上の懲役に処する。 一　外国（外国のために行動する者を含む。以下この条及び次条において同じ。）に通報する目的をもって、又は不当な方法で、防衛秘密を探知し、又は収集した者で、その探知し又は収集した防衛秘密を外国に通報した者 二　防衛秘密を取り扱うことを業務とし、又は業務としていた者で、その業務により知得し、又は領有した防衛秘密を外国に通報したもの 第五条　次の各号の一に該当する者は、二年以上の有期懲役に処する。 一　外国に通報する目的をもって、防衛秘密を探知し、又は収集した者 二　前条第一号又は第二号に該当する者を除き、防衛秘密を外国に通報した者 第六条　次の各号の一に該当する者は、十年以下の懲役に処する。 一　不当な方法で、防衛秘密を探知し、又	（罰則） 第四条　次の各号の一に該当する者は、死刑又は無期懲役に処する。 一　外国（外国のために行動する者を含む。以下この条、次条及び第六条において同じ。）に通報する目的をもって、又は不当な方法で、国家秘密を探知し、又は収集した者で、その探知し、又は収集した国家秘密を外国に通報して、我が国の安全を著しく害する危険を生じさせたもの 二　国家秘密を取り扱うことを業務とし、又は業務としていた者で、その業務により知得し、又は領有した国家秘密を外国に通報して、我が国の安全を著しく害する危険を生じさせたもの 第五条　次の各号の一に該当する者は、無期又は三年以上の懲役に処する。 一　外国に通報する目的をもって、又は不当な方法で、国家秘密を探知し、又は収集した者で、その探知し、又は収集した国家秘密を外国に通報したもの 二　国家秘密を取り扱うことを業務とし、又は業務としていた者で、その業務より知得し、又は領有した国家秘密を外国に通知したもの 三　前条第一号又は第二号に該当する者を除き、国家秘密を外国に通報した者 第七条　次の各号の一に該当する者は、十年以下の懲役に処する。 一　不当な方法で、国家秘密を探知し、又は

は収集した者

二　防衛秘密を取り扱うことを業務とし、又は業務としていた者で、その業務により知得し、又は領有した防衛秘密を他人に漏らしたもの

第七条　前条第二号に該当する者を除き、業務により知得し、又は領有した防衛秘密を他人に漏らした者は、五年以下の懲役に処する。

第八条　前四条の未遂罪は、罰する。

第九条　防衛秘密を取り扱うことを業務とし、又は業務としていた者で、その業務により知得し、又は領有した防衛秘密を過失により他人に漏らしたものは、二年以下の禁錮又は二十万円以下の罰金に処する。

第十条　第四条の罪の陰謀をした者は、十年以下の懲役に処する。

2　第五条の罪の陰謀をした者は、七年以下の懲役に処する。

3　第六条の罪の陰謀をした者は、五年以下の懲役に処する。

4　第七条の罪の陰謀をした者は、三年以下の懲役に処する。

5　第四条の罪を犯すことを教唆し、又はせん動した者は、第一項と同様とし、第五条の罪を犯すことを教唆し、又はせん動した者は、第二項と同様とし、第六条の罪を犯すことを教唆し、又はせん動した者は、第三項と同様とし、第七条の罪を犯すことを教唆し、又はせん動した者は、前項と同様とする。

6　前項の規定は、教唆された者が教唆に係る犯罪を実行した場合において、刑法（明治四十年法律第四十五号）総則に定める教唆の規定の適用を排除するものではない。

（自首減免）

第十一条　第五条第一号、第六条第一号、第八条又は前条第一項から第四項までの罪を犯した者が自首したときは、その刑を減軽し、又は免除する。

収集した者

二　国家秘密を取り扱うことを業務とし、又は業務としていた者で、その業務により知得し、又は領得した国家秘密を他人に漏らしたもの

第八条　前条第二号に該当する者を除き、国家秘密を他人に漏らした者は、五年以下の懲役に処する。

第九条　第五条（同条第三号に係る部分を除く。）及び前三条の未遂罪は、罰する。

第十条　国家秘密を取り扱うことを業務とし、又は業務としていた者で、その業務により知得し、又は領得した国家秘密を過失により他人に漏らしたものは、二年以下の禁錮又は二十万円以下の罰金に処する。

2　前項に該当するものを除き、業務により知得し、又は領有した国家秘密を過失により他人に漏らした者は、一年以下の禁錮又は十万円以下の罰金に処する。

第十一条　第五条（同条第三号に係る部分を除く。）の罪の予備又は陰謀をした者は、十年以下の懲役に処する。

2　第六条の罪の予備又は陰謀をした者は、七年以下の懲役に処する。

3　第七条の罪の陰謀をした者は、五年以下の懲役に処する。

4　第八条の罪の陰謀をした者は、三年以下の懲役に処する。

5　第五条（同条第三号に係る部分を除く。）の罪を犯すことを教唆し、又はせん動した者は、第一項と同様とし、第六条の罪を犯すことを教唆し、又はせん動した者は、第二項と同様とし、第七条の罪を犯すことを教唆し、又はせん動した者は、第三項と同様とし、第八条の罪を犯すことを教唆し、又はせん動した者は、前項と同様とする。

6　（同上）

（自首減免）

第十二条　第六条第一号、第七条第二号、第九条又は前条第一項から第四項までの罪を犯した者が自首したときは、その刑を減軽し、又は免除する。

（国外犯）

第十二条　第四条から第九条まで及び第十条第一項から第五項までの罪は、刑法第二条の例に従う。

（この法律の解釈適用）

第十三条　この法律の適用に当たっては、表現の自由その他国民の基本的人権を不当に侵害するようなことがあってはならない。

2　出版又は報道の業務に従事する者が、専ら公益を図る目的で、防衛秘密を公表し、又はそのために正当な方法により業務上行った行為は、これを罰しない。

附則

この法律は、公布の日から起算して六月を超えない範囲内において政令で定める日から施行する。

別表（第二条関係）

一　防衛のための態勢、能力若しくは行動に関する構想、方針若しくは計画又はその実施の状況

二　自衛隊の部隊の編成又は装備

三　自衛隊の部隊の任務、配備、輸送、行動又は教育訓練

四　自衛隊の施設の構造、性能又は強度

五　自衛隊の通信の内容

六　自衛隊の通信に用いる暗号

七　自衛隊の任務の遂行に必要な艦船、航空機、武器、弾薬、通信器材、電波器材その他の装備品及び資材（次号において「装備品等」という。）の構造、性能若しくは製作、保管若しくは修理に関する技術、使用の方法又は品目及び数量

八　自衛隊の任務の遂行に必要な装備品等の研究開発若しくは実験の計画、その実施の状況又はその成果

九　我が国の安全保障に係る外交上の方針

十　我が国の安全保障に係る外交上の方針

十一　我が国の安全保障に係る外交上の通信に用いる暗号

十二　我が国の安全保障に係る外国に関する情報

（国外犯）

第十三条　第四条から第十条まで及び第十一条第一項から第五項までの罪は、刑法第二条の例に従う。

（この法律の解釈適用）

第十四条　この法律の適用に当たっては、これを拡張して解釈して、国民の基本的人権を不当に害するようなことがあってはならない。

附則

（同上）

別表（第二条関係）

一　防衛のための態勢等に関する事項

イ　防衛のための態勢、能力若しくは行動に関する構想、方針若しくは計画又はその実施の状況

ロ　自衛隊の部隊の編成又は装備

ハ　自衛隊の部隊の任務、配備、行動又は教育訓練

ニ　自衛隊の施設の構造、性能又は強度

ホ　自衛隊の部隊の輸送、通信の内容又は暗号

ヘ　防衛上必要な外国に関する情報

二　自衛隊の任務の遂行に必要な装備品及び資材に関する事項

イ　艦船、航空機、武器、弾薬、通信器材、電波器材その他の装備品及び資材（以下「装備品等」という。）の構造、性能若しくは製作、保管若しくは修理に関する技術、使用の方法又は品目及び数量

ロ　装備品等の研究開発若しくは実験の計画、その実施の状況又はその成果

三　外交上の方針

イ　外交交渉の内容

ロ　外交上必要な外国に関する情報

ハ　外交上の通信に用いる暗号

ニ

2. 裁判例

（情報の不正取得・漏示に関する裁判例）

(1) コンピュータ情報

- 新潟鉄工所事件（東京地判昭60・2・13 刑裁月報17・1＝2・22）

＜新会社設立に伴うソフトウェアの横領＞

事実：社外でコピーするため、ソフトウェア開発グループのマネージャー（課長職）が、業務上保管中のシステム設計書・仕様書等を同グループ事務室から社外へ持ち出した。（業務上横領）

判示：他人の物を一時使用後返還する意思があったとしても、その間、所有権者を排除し自己の所有物と同様にその経済的用法にしたがってこれを利用しまたは処分する意図がある限り不法領得の意思が認められる。本件機密資料はその内容自体に経済的価値があり、かつ、所有者以外その許可なくコピーしえないものであるから、「被告人等が許可を受けずほしいまま本件資料をコピーする目的をもってこれを社外に持ち出すにあたっては、その間、所有者である新潟鉄工を排除し、本件資料を自己の所有物と同様にその経済的用法に従って利用する意図があったと認められる」。

- 綜合コンピュータ事件（東京地判昭60・3・6判時1147・162、判タ553・262）

＜転職に伴うソフトウェアの持ち出し＞

事実：自社が販売したコンピュータに新聞販売店購読者管理システムのプログラムを入力するなど、ユーザーに対するアフターサービスを担当していた者が、他社（被告人が転職しようとしていた会社）の納入したコンピュータに入力した。（背任）

判示：被告人は、会社の設置するコンピュータにのみプログラムを入力

する等、同社のため忠実にその業務を遂行すべき任務を有していたが、その任務に背き、自己らの利益を図る目的で、自己の管理するプログラムを会社に無断で他社の納入したコンピュータに入力し、自社にプログラム入力代金相当額の財産上の損害を与えた。

- 北海道銀行事件（札幌地判昭59・3・27 判時1116・143）

＜オンライン取引データの盗聴＞

事実：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うえ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 133万円を窃取した。（公衆電気通信法違反、窃盗）

判示：同法 112条所定の通信がデータ通信をも包含するものであることは、同法全体の文理上明らかであり、データ通信における通信の秘密の保護は、電信電話のそれに比して勝るとも劣らず重要なものであるから、以上の解釈は実質的に不合理をきたすものではない。

〔その他コンピュータ情報の不正取得・漏示が問題になった裁判例〕

	（客　体）
近畿相互銀行事件（大阪地判昭57・9・9刑裁月報14・10・776）	暗証番号
福岡銀行通帳偽造事件	暗証番号
軽自動車協会連合会事件（東京地判昭61・9・8）	登録者名簿
京王百貨店事件（東京地判昭62・9・30 判時1250・144）	顧客名簿

(2) マニュアル情報

- 大日本印刷事件（東京地判昭40・6・26 下刑集7・6・1319）

＜社内で作成したコピーの所有権関係＞

事実：総務部第2課副課長が、稟議決裁一覧表原本を技術部から借りだし、総務部備付の感光紙に複写して社外に持ち出した。（窃盗）

判示：社内で、「ほしいままに、同社の機密書類を同社所有の感光紙に同社の複写器を使って複写し、これを社外に持ち出したものであるから、全体的にみて、単なる感光紙の窃盗ではなく、同社所有の複写した右稟議決裁一覧表を窃取したものと認めるのが相当である」。

＜不法領得の意思関係＞

事実：総務部秘書課雇が秘書課長保管の大口受註報告書1228枚等を会社から持ち出した。（窃盗）

判示：廃棄処分されるまでは総務課内のロッカーに厳重に保管されるべきであったものを、「第三者に渡すため無断搬出することがその権利者（所有者ないし占有者）を排除し、自己が完全な支配を取得する行為であること〔を、行為者は〕当然理解していた」。

- 建設調査会事件（東京地判昭55・2・14 刑裁月報12・1＝2・47）

＜コピー目的の資料一時持出と領得意思＞

事実：業務部長が、総務部業務係保管の購読会員名簿4冊を社外に持ち出し、コピーして2時間後に元の机引出内に戻した。（窃盗）

判示：「本件購読会員名簿の経済的価値は、それに記載された内容自体にあるものというべく、この内容をコピーし、それを自社と競争関係に立つ会社に譲り渡す手段として、本件購読会員名簿を〔本件〕態様により利用することの意思は、権利者を排除し、右名簿を自己の所有物と同様にその経済的用法に従い利用する意思であ

つたものと認めるのが相当である。」

- 東洋レーヨン事件（神戸地判昭56・3・27 判時1012・35）

＜守秘義務と背任罪における任務違背＞

事実：ナイロン糸製造工程及び装置の開発改善に従事する東レA工場技術工務課副部員が、同社他工場のポリエステル製造装置、テトロンフィルム製造装置等に関する秘密資料（設計図等）を、他工場の保管部局の職員を欺罔して借り出し、またはA工場に参考資料として送付されてきたときに無断で持ち出し、これを写真撮影し、競争会社に売却した。（背任）

判示：本件各資料は、被告人が本来副部員たる地位に基づく担当事務の処理として入手したわけではないから、担当事務の処理のために入手したものについて保管秘匿の任務を有するのと同一に考えることはできない。また、被告人は「就業規則等に基づいて東レ所有の秘密を保管し、これを社外に漏らしてはならない義務を負担しており、被告人Sの本件各所為は、かような義務に違反する側面を有するけれども、かような義務は、同被告人の担当事務との関係の有無を問わず存在するものであって、かような義務違反は、雇用契約に基づく一般的忠実義務違反としての責任を生じることはあっても刑法 247条の背任罪にいう事務処理についての任務違背として評価することはできない。」（なお、被告人の所為は、窃盗ないし詐欺罪を構成する可能性がある。）

- 新薬産業スパイ事件（富山化学）(東京地判昭59・6・15 刑裁月報16・5＝6・459)

＜コピー目的の資料一時持出と領得意思＞

事実：国立予防衛生研究所抗生物質製剤室勤務の厚生技官が、コピーし

て直ちに返還する意思で、同室長の専用戸棚から新薬製造承認申請書等のファイル1冊を取り出した。（窃盗）

判示：「本件各資料の経済的価値がその具現化された情報の有用性、価値性に依存するものである以上、資料の内容をコピーしその情報を獲得しようとする意思は、権利者を排除し右資料を自己の物と同様にその経済的用法に従って利用する意思にほかならないと言うべきであるから、」被告人には領得意思があったと認められる。資料を返還する意思が犯行時に存在したことは、不法領得の意思の存在に影響を及ぼすものではない。

- 新薬産業スパイ事件（帝三製薬）(東京地判昭59・6・28 刑裁月報16・5＝6・476)

＜コピー目的の資料一時持出と領得意思＞

事実：国立予防衛生研究所抗生物質製剤室勤務の厚生技官が、T社社員に渡してコピーさせるため、同室長の専用戸棚からM社開発新薬に関する資料・製造承認申請書等のファイル1冊を取り出した。（窃盗）

判示：本件ファイルの財物としての価値は、情報が化体されているところにあるとともに、権利者以外の者の利用が排除されていることにより維持されているのであるから、情報を複写して複写媒体を手元に残すことは、原媒体ともいうべきファイルそのものを窃かに権利者と共有し、ひいては自己の所有物とするのと同様の効果を挙げることができる。これは、権利者でなければ許されないことである。しかも、ファイルが返還されたとしても、権利者の独占的・排他的利用は阻害され、ファイルの財物としての価値は大きく減耗する。本件被告人は、ファイルを複写して情報を自らのものとし、このような効果を狙う意図・目的のために持ち出した

のであるから、権利者を排除し本件ファイルを自己の所有物と同様にその経済的用法に従い利用または処分する意思があったと認められる。複写後速やかに返還し、その間の権利者の利用を妨げない意思であり、物理的損耗も伴わないものであっても、領得意思を認めざるをえない。

〔その他マニュアル情報の不正取得・漏示が問題になった裁判例〕

	（客　体）
鐘淵化学事件（大阪地判昭42・5・31 判時494・74）	技術資料
早大入試事件（東京高判昭56・8・25 判時1032・139）	試験問題

（注）以上63年度日本刑法学会レジュメ等より引用

3．海外法制

西ドイツ刑法　（１９８６年改正）

（データの探知）

第２０２条ａ

（１）　自己の用に供するものでなく，かつ，無権限のアクセスに対して特別に保護されているデータを，権限なく取得し，又は他人をしてこれを取得せしめた者は，３年以下の自由刑又は罰金に処する。

（２）　前項において「データ」とは，電子的，電磁的，又はその他直接に知覚できない方法で蓄積され，又は伝達されるもののみをいう。

（コンピュータ詐欺）

第２６３条ａ

（１）　財産上不法の利益を得，又は他人をしてこれを得せしめる目的で，プログラムの虚偽作成，虚偽のデータ若しくは不完全なデータの使用，データの無権限使用その他プロセス（Ａｂｌａｕｆ）に対する無権限の作用によりデータ処理過程の結果に影響を及ぼすことによって，他人の財産に損害を加えた者は，５年以下の自由刑又は罰金に処する。

（２）　前項の場合においては，第２６３条第２項から第５項までを準用する。

（技術的記録の偽造）

第２６８条・・・１９６９年改正により新設

（１）　法律上の取引において他人を欺罔するため，

１　真正でない技術的記録を作成し，若しくは技術的記録を変造した者，又は

２　真正でない技術的記録若しくは変造の技術的記録を行使した者

は，５年以下の自由刑又は罰金に処する。

（２）　技術的記録とは，データ，測定値若しくは計算値，状態，又は出来事の推移の叙述であって，技術的機械によりその全部又は一部が自動的に記録され，記録の対象を一般に又は専門家に認識させ，かつ法的に重要な事実の証明に予定されているものをいう。ただし，作成の際に上のように予定されたか，後になって予定されたかを問わない。

（３）　行為者が記録の過程に妨害的に干渉することによって記録の結果に影響を与えたときも，真正でない技術的記録の作成と同等とする。

（４）　本条の罪の未遂罪は，これを罰する。

（５）　第２６７条第３項の規定は，これを適用する。（特に重い事態においては，その刑は１年以上の自由刑とする。）

（事実証明に関するデータの偽造）

第２６９条

（１）　法律上の取引において他人を欺罔するため，事実証明に関するデータを，見読可能な状態にすれば偽造文書若しくは変造文書となるように蓄積し若しくは変更し，又はこのようにして蓄積され若しくは変更されたデータを使用した者は，５年以下の自由刑又は罰金に処する。

（２）　前項の未遂罪は，罰する。

（３）　第２６７条第３項を適用する。（特に重い事態においては，その刑は１年以上の自由刑とする。

（データ処理の際の法律上の取引の欺罔）

第２７０条

法律上の取引においてデータ処理に誤った影響を与えることは，法律上の取引における他人の欺罔とみなす。

（間接的な虚偽（公）文書作成）

第２７１条

（１）　権利又は権利関係にとって重要な意思表示，交渉又は事実が，全く行われず若しくは発生せず，又は他の方法で若しくは無資格者によって若しくは他の者によって行われ若しくは発生しているにもかかわらず，公の文書，帳簿，記録（Ｄａｔｅｉｅｎ）又は登録簿において，それが行われ又は発生したものとして記載され又は蓄積される結果を生ぜしめた者は，１年以下の自由刑又は罰金に処する。

（虚偽（公）文書の行使）

第２７３条

第２７１条の虚偽の記載がなされ又はデータ蓄積がなされたものを行使した者は，第２７１条の刑を科する。

（文書隠匿，境界表示の変更）

第２７４条

（１）　次の者は，５年以下の自由刑又は罰金に処する。

１　自己に属しないか，若しくは専ら自己のみには属しない文書若しくは技術的記録を，他人に不利益を与える目的で，破棄し，毀損し若しくは隠匿した者

２　自己が処分しえないか，若しくは単独では処分しえない事実証明に関するデータ（第２０２条ａ第２項）を，他人に不利益を与える目的で，消去し，隠匿し，使用不能にし若しくは改変した者，又は

３　（略）

（２）　前項の未遂罪は，罰する。

（データの改変）

第３０３条ａ

（１）　不法にデータ（第２０２条ａ第２項）を消去し，隠匿し，使用不能にし又は改変した者は，２年以下の自由刑又は罰金に処する。

（２）　前項の未遂罪は，罰する。

（コンピュータ・サボタージュ）

第３０３条ｂ

（１）　他の経営体若しくは企業又は官庁にとって重要な意義を有するデータ処理を次に掲げる行為によって妨害した者は，５年以下の自由刑又は罰金に処する。

１　第３０３条ａ第１項に規定する行為を行うこと

２　データ処理装置又はデータ媒体を破壊し，損壊し，使用不能にし，取り除き，又は改変すること

（２）　前項の未遂罪は，罰する。

（告訴）

第３０３条ｃ

第３０３条から第３０３条ｃまでの罪については，告訴をまってこれを論ずる。ただし，刑事訴追について特別な公益が存するために，刑事訴追官庁が職権による訴追の開始を必要と認めるときは，この限りでない。

（職務上の不実記載）

第３４８条

（１）　公文書を作成する権限を有する公務員が，その権限の範囲内で，法律的に重要な事実について虚偽の記載をし，又は公の登録簿，帳簿若しくは記録（Ｄａｔｅｉｅｎ）に虚偽の記入をし，若しくは虚偽の入力をしたときは，５年以下の自由刑又は罰金に処する。

不正競争防止法第一七条　営業上・経営上の秘密の保護　(1)ある業務体の従業員、労働者または徒弟として、雇用関係にもとづいて自己に打ち明けられまたは得るところとなった営業上または経営上の秘密を、雇用関係の継続期間中に、競業の目的で、または自己の利益を図るために、または第三者のために、またはその事業主に損害を与える目的で、権限なくある者に知らせた者は、三年以下の自由刑または罰金に処する。

(2)競業の目的で、または自己の利益を図るために、または第三者のために、またはその事業主に損害を与える目的で、

一　営業上もしくは経営上の秘密を、

a　技術的な手段を用いること

b　秘密が化体された複製物（Wiedergabe）を作成すること、もしくは

c　秘密が化体された物を奪取すること

により権限なく入手しもしくは確保（sichern）した者、

または

二　第一項に定められた漏示行為により、もしくは第一号にあたる自己もしくは他人の行為により獲得した営業上もしくは経営上の秘密、もしくはそのほかの方法で権限なく入手しもしくは確保した営業上もしくは経営上の秘密を、権限なく利用しもしくはある者に知らせた者

も前項と同様に処罰される。

(3)この罪の未遂犯は、これを罰する。

(4)特に重い事例においては、刑は五年以下の自由刑または罰金とする。行為者が漏示行為にあたり、秘密が外国において利用されることを知っていた場合、または、行為者がその秘密をみずから外国で利用した場合には、原則として特に重い事例となる。

井田良「西ドイツにおけるコンピュータ犯罪処罰規定とデータの保護」刑法雑誌二八巻四号収録

情報処理関連不正行為に関する一九八八年一月五日の法律第八八―一九号（Loi n° 88―19 du 5 janvier 1988 relative à la fraude informatique）

唯一条文　刑法典第三部第二編中、第二章の後に、次の第三章を挿入する。

第三章　ある種の情報処理関連犯罪

第四六二条の二　不正に、自動情報処理システムの全体もしくは一部にアクセスし、または、そのシステムの中にとどまった者は、二月以上一年以下の拘禁刑および二千フラン以上五万フラン以下の罰金刑に処し、または、これらいずれかの刑に処する。右の行為により、同システム中に収納された情報の消去もしくは改変、または、同システムの動作（fonctionnement）の悪化を生じさせたときは、本条の拘禁刑は二月以上二年以下とし、罰金刑は一万フラン以上一〇万フラン以下とする。

第四六二条の三　故意に、他人の権利を害して、自動情報処理システムの動作を妨害（entrave）し、または狂わせた（fausser）者は、三月以上三年以下の拘禁刑および一万フラン以上一〇万フラン以下の罰金刑に処し、または、これらいずれかの刑に処する。

第四六二条の四　故意に、他人の権利を害して、直接的または間接的に、自動情報処理システムにデータを入力し、または同システムに収納されたデータもしくは処理、伝送に関する方法（mode）を消去もしくは改変した者は、三月以上三年以下の拘禁刑および二千フラン以上五〇万フラン以下の罰金刑に処し、または、これらいずれかの刑に処する。

第四六二条の五　形式の如何を問わず、コンピュータ記録（documents informatisés）に、他人に損害を与えるような性質の偽・変造（falsification）を行なった者は、一年以上五年以下の拘禁刑および二万フラン以上二〇〇万フラン以下の罰金刑に処する。

第四六二条の六　情を知って（sciemment）、前条の客体たるコンピュータ記録を行使した者は、一年以上五年以下の拘禁刑および二万フラン以上二〇〇万フラン以下の罰金刑に処し、またはこれらいずれかの刑に処する。

第四六二条の七　第四六二条の二ないし前条に掲げる罪の未遂は、各罪（の既遂）と同一の刑に処する。

第四六二条の八　第四六二条の二ないし前条に掲げる内の一つもしくは複数の罪に関する、一つもしくは複数の有形的な行為により具体化された準備（préparation）を目指して形成された合意（association）または成立した共謀（entente）に加担した者は、各罪について定められた刑または最も重く罰せられる罪について定める刑に処する。

第四六二条の九　裁判所は、有罪の言渡しを受けた者に帰属し、本章に規定する罪を犯すために用いられた機器（matériel）の没収を言い渡すことができる。

フランス刑法研究会「フランスにおけるコンピュータ犯罪（三）」
国学院法学二六巻一号収録

（フランス）

一九八六年刑法改正草案（廃案）

第七章　コンピュータ関連犯罪（Les infractions en matière informatique）

第三〇七条の一　自動情報処理システムのプログラム、データ、またはその他すべての情報を不法に取得する行為は、拘禁刑三年および罰金一〇〇万フランで罰せられる。

第三〇七条の二　他人の権利を害して（au mépris des droits d'autrui (12)）、自動情報処理システムのプログラム、データ、またはその他すべての情報を使用し、伝送し、または複製する行為は、拘禁刑三年および罰金一〇〇万フランで罰せられる。

第三〇七条の三　故意に、他人の権利を害して、自動情報処理システムの全部または一部を破壊もしくは改変し、またはその機能を阻害し、もしくは誤らせる行為は、拘禁刑五年および罰金二五〇万フランで罰せられる。

第三〇七条の四　自動情報処理システムを不法に使用することによって、違法な利益を得、または他人をしてこれを得させる行為は、拘禁刑五年および罰金二五〇万フランで罰せられる。

＊法案は、以上の四つの犯罪類型を規定し、続く第三〇七条の五から同条の八までの条項で、本章の罪につき、公民権停止、職業禁止、没収、事業所閉鎖、取引停止、手形・小切手の振り出し禁止などの多様な付加的刑罰を規定し、また、法人処罰と未遂犯の処罰を定めている。

南部篤「フランスのコンピュータ犯罪と刑法」
法学紀要二十九巻収録

フランス 1986 年　刑法典改正法案（廃案）

〔第２部　人に対する重罪と軽罪、第６章人格への侵害〕

第四節　秘密の侵害

第一項　職業上の秘密の侵害

第二二六－一三条　身分もしくは職業により、職務もしくは一時的任務を理由として秘密の性格を有する情報の保有者となった者が秘密を共有する資格のない者にその情報を故意に漏らしたとき、その者は一年の拘禁および三〇万フランの罰金により罰せられる。

②訴追は、被害者・その法定代理人またはその権利承継人の告訴に基づいてのみ提起されうる。ただし、訴追が開始されたのちは、それを告訴の取消（retrait）によって消滅させることはできない。

第二二六－一三条　第二二六－一二条の規定は、法律が秘密の顕示を課すときまたは許可するとき、適用されない。さらに、次の者に対しても適用されない。

一　一五歳未満の未成年者または年齢もしくは身体的・精神的状態により自らを保護できない者に対し加えられた虐待または窮乏状態（privations）を認知し、それを司法・医療または行政機関へ通知する者

二　職業の遂行中に確認したなんらかの性質の性的暴行が行なわれたことの推定を可能にする虐待を、被害者の同意を得て、検察官に通告する医師

第二項　人名情報（informations nominatives）の保護

第二二六－一四条　情報処理（informatique）・情報ファイル（fichiers）および自由に関する法律第二五条第二六条および第二八条から第三一条の定める収集・登録および保存に関する規則に違反して、人名情報を記録し・記録させ・保存し・保存させる行為は、五年の拘禁および二〇〇万フランの罰金により罰せられる。

第二二六－一五条　記録・分類・伝達またはその他の形式の処理の際に人名情報を保持した者のいずれかによる、情報処理・情報ファイルおよび自由に関する法律の適用により定義される目的から逸脱してそれらの情報を利用する（détourner）行為は、五年の拘禁および二〇〇万フランの罰金により罰せられる。

第二二六－一六条　記録・分類・伝達またはその他の形式の処理の際に、その公表が結果として利害関係人の評判または私生活の内面に侵害をもたらす人名情報を収集した者のいずれかによる、利害関係人の許可のないにもかかわらず、受け取る資格のない第三者にそれらの情報を故意に知らせる行為は、一年の拘禁および一〇万フランの罰金により罰せられる。

第三項　通信の秘密の侵害

第二二六－一七条　宛て先に到達しているか否かを問わず第三者に宛てた通信物を、悪意により（de mauvaise foi）、開封し、その到着を遅らせまたはそれを横領する行為は、一年の拘禁および一〇万フランの罰金により罰せられる。

②悪意により、電気通信（télécommunications）手段により発信され、伝達されまたは受信された通信の内容を知り、それを横領しまたはその内容を改変する行為は、同じ刑罰により罰せられる。

（恒光　徹訳・岡山大学法学会雑誌 37 巻 4号）

第21章　アクセスの企て（access devices）及びコンピュータ

第2101

この章は、「虚偽のアクセスの企て並びにコンピュータ詐欺及び盗用に関する1984年法」として引用され得る。

第2102条

(a)　この合同決議第16章により改正された連邦法典第18編第47章の末尾に、さらに次の条項を加える。

「（コンピュータに関係する詐欺及び関連行為）
第1030条」

「(a)　何人といえども、

(1)　権限がないことを知りながらコンピュータにアクセスし、又はコンピュータにアクセスする権限を盗用して、当該権限が許容しない目的のためにアクセスの機会を利用し、当該行為により、連邦を害し若しくは外国の利益を図るために当該情報を使用する意図又はそのように信ずべき理由を持って、連邦政府が行政命令若しくは法令により国防上若しくは外交上の理由に基づき無権限の開示を禁じた情報若しくは1954年原子力法第11条(r)項に規定する非公開の情報を得た者、

(2)　権限がないことを知りながらコンピュータにアクセスし、若しくは、コンピュータにアクセスする権限を盗用して、当該権限が許容しない目的のためにアクセスの機会を利用し、当該行為により、1978年金融プライバシー権法（the Right to Financial Privacy Act of 1978 12 U. S. C. 3401以下）に規定する金融機関の金融記録、若しくは、公正信用報告法（the Fair Credit Reporting Act 15 U. S. C. 1681以下）に規定する消費者信用情報機関（consumer reporting agency）の消費者に関するファイルに含まれた情報を得た者、又は

(3)　権限がないことを知りながらコンピュータにアクセスし、若しくは、コンピュータにアクセスする権限を盗用して、当該権限が許容しない目的のためにアクセスの機会を利用し、当該行為により、連邦政府により又は連邦政府のために運用されるコンピュータ内の情報を故意に使用し、改ざんし、破壊し若しくは開示し、又はコンピュータの正当な使用を妨げ、連邦政府のコンピュータの運用に影響を与えた者は、

本条(c)項に規定するところにより処罰される。但し、コンピュータにアク

セスする権限を有する者が、かかるアクセスの許容しない目的のためにアクセスの機会を利用した場合において、それが単なるコンピュータの使用にとどまるときは、(2)号又は(3)号に規定する罪とはならない。」

「(b)(1) 本条(a)項の罪の未遂は、本条(c)項に規定するところにより処罰される。

(2) 本条(a)項の罪を実行するため２名以上の者で共謀し、その構成員が同罪の実現のために何らかの行為を行ったときは、本条(c)項が規定する最高額を超えない罰金若しくは同項が規定する長期の２分の１以下の拘禁刑に処し、又はこれを併科する。」

「(c) 本条(a)項又は(b)項(1)号の罪に対する処罰は、

(1)(A) 本条(a)項(1)号の犯罪であって、以前に同号の罪につき有罪とされたことがない場合、又は本号によって処罰される犯罪の未遂の場合は１万ドル若しくは犯罪によって得た価値の２倍のいずれか大きい額以下の罰金若しくは10年以下の拘禁刑に処し、又はこれを併科する。

(B) 本条(a)項(1)号の犯罪であって、以前に同号の罪につき有罪とされたことがある場合、又は本号によって処罰される犯罪の未遂の場合は10万ドル若しくは犯罪によって得た価値の２倍のいずれか大きい額以下の罰金若しくは20年以下の拘禁刑に処し、又はこれを併科する。

(2)(A) 本条(a)項(2)号又は３号の犯罪であって、以前に右各号の罪につき有罪とされたことがない場合、又は本号によって処罰される犯罪の未遂の場合は5,000ドル若しくは犯罪によって得た若しくは減殺した価値の２倍のいずれか大きい額以下の罰金若しくは１年以下の拘禁刑に処し、又はこれを併科する。

(B) 本条(a)項(2)号又は(3)号の犯罪であって、以前に右各号の罪につき有罪とされたことがある場合、又は本号によって処罰される犯罪の未遂の場合は１万ドル若しくは犯罪によって得た若しくは減殺した価値の２倍のいずれか大きい額以下の罰金若しくは10年以下の拘禁刑に処し、又はこれを併科する。」

「(d) 連邦シークレット・サービスは、権限を有する他の機関と同様、本条に規定する犯罪について捜査を行う権限を有する。連邦シークレット・サービスのかかる権限は、財務長官及び司法長官（the Secretary of the Treasury and the Attorney General）の合意するところに従って行使されなければならない。」

「(e) 本条において「コンピュータ」とは、論理演算、算術演算若しくは記憶機能を有する電気的、磁気的、光学的、電子化学的（electrochemical）又はその他の高速データ処理装置を意味し、かかる装置と直結し又は連結して運用されるデータ記憶装置又は通信装置を含むが、自動タイプライター若しくは植字機、携帯用小型計算機（portable hand head calculator）又はその他この種の装置を含まない。」

(b) 連邦法典第18編第47章の冒頭の条文目次の末尾に、新たに次の項目を加える。
「第1030条　コンピュータに関する詐欺及び関連行為」

第2103条

司法長官は、本合同決議の制定の日から3年間、議会に対し、本章により追加された連邦法典第18編中の各条に基づく訴追に関する報告を毎年行わなければならない。

＊　1986年改正による追加規定

第1030条(a)

(4) 故意かつ欺罔の目的で、権限なく、又はアクセスの権限を越えて連邦関係コンピュータ(a Federal interest computer) にアクセスし、かつ当該行為により、目的とする詐欺行為を推進し、価値あるもの(anything of value) を取得すること。ただし、詐欺の客体、取得されたものがコンピュータの使用にすぎないときを除く。

(5) 故意に無権限で連邦関係コンピュータにアクセスし、一回以上の当該行為により、当該連邦関係コンピュータの情報を改変、損傷若しくは破壊し、又は当該コンピュータ若しくは情報の権限ある者による利用を妨げ、かつそれにより、

(A) 一人以上の他人に、一年間に、合計千ドル以上の価値の損害を与えること、又は、

(B) 一人以上の個人の診察、診断、治療又はケアを変更若しくはそこない、又は部分的に変更若しくはそこなうこと。

(6) 故意にかつ詐欺の目的で、コンピュータに権限なくアクセスできるようなパスワードまたは同様の情報を取り引き（譲渡・売却または譲渡・売却の意思で自己の支配下におくこと）すること。ただし、

(A)当該取り引きが州際通商または国際通商に影響を及ぼし、又は、

(B)当該コンピュータが連邦政府により、または連邦政府のために使用される場合に限る。

（定義）

第５０２条

(a) 本条において，次の各号に掲げる用語の意義は，それぞれ当該各号に定めるところによる。

(1) アクセス　コンピュータ・システム又はコンピュータ・ネットワークに命令すること，それらをもって通信すること，それらにデータを記憶させること又はそれらからデータを検索することをいう。

(2) コンピュータ・システム　一個の装置又は数個の装置の集合であって，論理，演算，データの記憶及び検索，通信並びに制御（ただし，これらに限らない）の機能を果たすものをいう。ただし，プログラミングができず，少なくとも１がコンピュータ・プログラム及びデータを包含する外部のファイルと接続して使用することのできないポケット計算機は除く。

(3) コンピュータ・ネットワーク　２以上のコンピュータ・システムの相互連絡をいう。

(4) コンピュータ・プログラム　コンピュータ・システムにおいてそのままの形態又は修正された形態で自動的に操作された場合に，コンピュータ・システムに特別な機能を果たせる命令又はステートメント及び関連データの系統的組合せをいう。

(5) データ　定型化した様式で作成されつつあるか，又は作成され，コンピュータ・システム又はコンピュータ・ネットワークにおいて使用することを意図している情報，知識，事実，概念又は命令の表象をいう。

(6) 商業証券　小切手，為替手形，権利証書，為替，約束手形，預金証書，信用状，外国貿易用為替手形，クレジット（デビット）カード，トランスアクションオーソライゼイションメカニズム，市場性のある保証，又はそれらのコンピュータ・システム表示を含むが，それらに限定されない。

(7) 財産　人間及びコンピュータ・システムが読むことのできるデータ及び伝送中のデータを含め，有体であると無体であるとを問わず，商業証券，データ，コンピュータ・プログラム，並びにコンピュータ・システム及びコンピュータ・プログラムに関連する資料，又はそれらのコピーを含むが，それらに限定されない。

(8) サービス　コンピュータ・システム，コンピュータ・ネットワーク，コンピュータ・プログラムの各利用，又はコンピュータ使用のために準備されたデータ，コンピュータ・システム内に含まれているデータ若しくはコンピュータ・ネットワーク内に含まれているデータの各利用を含むが，それらに限定されない。

(b) (1) 欺罔若しくは強要して財産を取得する計画若しくは策略を企て，若しくは実行するために，又は，(2) 虚偽若しくは詐欺的な意図，申立て若しくは約束により金銭，財産若しくはサービスを得るために，コンピュータ・システム又はコンピュータ・ネットワークに故意にアクセスし，又はアクセスさせた者は犯罪を犯したものである。

(c) 入手・利用の認められない他人の信用情報を得るために，悪意でコンピュータ・システム若しくはコンピュータ・ネットワークにアクセスし，若しくはアクセスさせた者，又は人の信用評価を不当に損ない，若しくは不当に高めるために，コンピュータ・システム若しくはコンピュータ・ネットワークに虚偽の情報を挿入し，若しくは挿入させた者は犯罪を犯したものである。

(d) コンピュータ・システム，コンピュータ・ネットワーク，コンピュータ・プログラム，又はデータに悪意でアクセスし，これを改変し，抹消し，損傷し，破壊し，又はその作動を中断させた者は犯罪を犯したものである。

(e) アクセスが許されていないことを知りながら，故意に，かつ，無権限で，コンピュータ・システム，コンピュータ・ネットワーク，コンピュータ・プログラム又はデータにアクセスした者は犯罪を犯したものとする。本項は，雇用の範囲内で行う限りは，雇主のコンピュータ・システム，コンピュータ・ネットワーク，コンピュータ・プログラム又はデータにアクセスする者に適用してはならない。

(f) (b) 項，(c) 項又は(d) 項の規定に違反した者は，１万ドル以下の罰金，16月間，２年間若しくは３年間の州刑務所内での拘禁，若しくはそれらの罰金刑と拘禁刑の併科，又は 5,000ドル以下の罰金，１年以下の郡刑務所内での拘禁，若しくはそれらの罰金刑と拘禁刑の併科をもって処罰する。ただし，他に別様に規定しているときは，この限りではない。

(g) (1) (e) 項の最初の違反で，損害が生じなかったときは，２５０ドル以下の罰金をもって処罰する違反である。

(2) (e) 項の違反で，損害が生じたとき，又は損害は伴わないが(e) 項の違反が２度目以上であるときは，5,000ドル以下の罰金，１年以下の郡刑務所内での拘禁，又はそれらの罰金刑と拘禁刑の併科をもって処罰する軽罪である。

(3) 本項において「損害」とは，コンピュータ・システム，コンピュータ・ネットワーク，コンピュータ・プログラム若しくはデータの改変，抹消，損傷若しくは破壊であって，アクセスによって生じたもの，又は，コンピュータ・システム，コンピュータ・ネットワーク，コンピュータ・プログラム若しくはデータがアクセスによって，改変，抹消，損傷若しくは破壊を受けなかったことを確かめるために所有者若しくは借主が負担したことに合理性及び必要性のある支出をいう。

(h) 略

(i) 本条はいかなる行為にも適用され又は適用され得る当州の刑法の他の条文の適用を排除するものと解釈してはならない。

フロリダ州法（１９７８年改正）

（略称）

第 815.01 条

本法の規定は「フロリダ・コンピュータ犯罪法」と称し，かつ引用することができる。

（立法目的）

第 815.02 条

州議会は次のように認定し，かつ宣言する。

(1) コンピュータ関連犯罪は，政府においても民間においてもますます問題となってきている。

(2) コンピュータ犯罪の被害は，その他のホワイトカラー犯罪に関連する被害に比して，１件当たりはるかに大きくなる傾向があるため，コンピュータ関連犯罪は公共に多大の被害をもたらす。

(3) コンピュータ・システムへの虚偽の記録のそう入，コンピュータ設備の無権限使用，コンピュータ化された情報又はファイルの改変又は損壊，並びに商業証券，データ及びその他の財産の窃取による金融機関，政府のプログラム，政府の記録及びそのほかの企業におけるコンピュータ関連犯罪の機会は非常に大きい。

(4) 種々の形態のコンピュータ犯罪は他の法規に基づき刑事訴追の対象となりうるとしても，種々の形態のコンピュータ乱用を禁止する，補充的，追加的法律を制定することは適切で望ましい。

（定義）

第 815.03 条

他の意味を示していることが明らかな場合を除き，本章において，次の各号に掲げる用語の意義は，それぞれ当該各号に定めるところによる。

(1) 知的財産　データをいい，プログラムを含む。

(2) コンピュータ　データ処理を行うように内部にプログラムされた自動装置をいう。

(3) 欠

(4) コンピュータ・ソフトウェア　コンピュータ・システムの運用に関する１組のコンピュータ・プログラム，手続及び関係資料をいう。

(5) コンピュータ・システム　１組の関連した，連結又は非連結のコンピュータ設備，装置又はコンピュータ・ソフトウェアをいう。

(6) コンピュータ・ネットワーク　通信設備を通じて互いにデータを伝送できる能力を備えた２以上のコンピュータ・システムを含む１組の，関連し遠隔的に連結された装置と通信設備をいう。

(7) コンピュータ・システム・サービス　有効な仕事を行うためにコンピュータ・システム又はコンピュータ・ネットワークを提供することをいう。

(8) 財産　第 812.011条に定義する価値あるすべてのものをいい，商業証券，電子的に作成されたデータ，機械が解読できるか又は人間が解読できるコンピュータ・ソフトウェア及びプログラムをも含む

情報，並びにその他何らかの有形又は無形の価値あるものを含むが，これらに限定されない。

(9) 商業証券　小切手，手形，為替，預金証書，信用状，外国貿易用為替手形，クレジット・カード又は流通証券をいう。

(10) アクセス　コンピュータ，コンピュータ・システム又はコンピュータ・ネットワークの装置に対し接近し，命令し，それらを使って通信し，それらにデータを蓄積し，それらからデータを検索し，又はそのほかの使用を行うことをいう。

（知的財産を侵害する罪）

第 815.04 条

(1) コンピュータ，コンピュータ・システム又はコンピュータ・ネットワークの内部若しくは外部に備えられ，又は存在するデータ，プログラム又は補助資料を，故意かつ無権限で変更した者は知的財産を侵害する罪を犯したものとする。

(2) コンピュータ，コンピュータ・システム又はコンピュータ・ネットワークの内部若しくは外部に備えられ，又は存在するデータ，プログラム又は補助資料を，故意かつ無権限で損壊した者は知的財産を侵害する罪を犯したものとする。

(3) コンピュータ，コンピュータ・システム又はコンピュータ・ネットワークの内部若しくは外部に備えられ，又は存在する，第 812.081条に定義する，企業秘密に当たり，又は法律により秘密とされるデータ，プログラム若しくは補助資料を，故意かつ無権限で，開示し，又は取得した者は知的財産を侵害する罪を犯したものとする。

(4)(a) 本項中に別に定めるところのほか，知的財産を侵害する罪は，第 775.082条，第 775.083条，又は第 775.084条に定めるところに従い処罰される，第３級の重罪となる。（※１）

(b) それが財産を騙取し又は取得するための計画又は策略を企て又は実行するために犯された場合は，その者は，第 775.082条，第 775.083条又は第 775.084条に定めるところに従い処罰される，第２級の重罪となる。（※２）

（コンピュータの装置又は用品に対する罪）

第 815.05 条

(1)(a) コンピュータ，コンピュータ・システム又はコンピュータ・ネットワークに使用し，又は使用する予定の装置又は用品を，故意かつ無権限で変更した者はコンピュータの装置又は用品に対する罪を犯したものとする。

(b)1. 本項中に別に定めるところのほか，本項(a) に定めるコンピュータの装置又は用品に対する罪は，第 775.082条，第 775.083条又は第 775.084条に定めるところに従い処罰される，第１級の軽罪となる。（※３）

2. それが財産を騙取し，又は取得するための計画又は策略を企て又は実行するために犯された場合は，その者は，第 775.082条，第 775.083条又は第 775.084条に定めるところに従い処罰される，第３級の重罪となる。

(2)(a) コンピュータ，コンピュータ・システム若しくはコンピュータ・ネットワークに使用し若しくは使用する予定の装置若しくは用品を，故意かつ無権限で破壊，取得，侵害若しくは損傷した者，又は，コンピュータ，コンピュータ・システム若しくはコンピュータ・ネットワークを，故意かつ無権限で破壊し，侵害し若しくは損傷した者は，コンピュータの装置又は用品に対する罪を犯したものとする。

(b)1. 本項中に別に定めるところのほか，本項(a)に定めるコンピュータの装置又は用品に対する罪は，第 775.082条，第 775.083条又は第 775.084条に定めるところに従い処罰される，第１級の軽罪となる。

2. コンピュータ装置若しくは用品に対する，又はコンピュータ，コンピュータ・システム若しくはコンピュータ・ネットワークに対する損害が２００ドルを超え１，０００ドル未満である場合は，その者は第 775.082条，第 775.083条又は第 775.084条に定めるところに従い処罰される，第３級の重罪となる。

3. コンピュータの装置若しくは用品に対する，若しくはコンピュータ，コンピュータ・システム若しくはコンピュータ・ネットワークに対する損害が１，０００ドル以上である場合，又は，公務若しくは公共通信，運輸若しくは水，ガス若しくはその他の公共サービスの供給が妨害され，若しくは減損した場合は，その者は第 775.082条，第 775.083条又は第 775.084条に定めるところに従い処罰される，第２級の重罪となる。

（コンピュータ利用者に対する罪）

第 815.06 条

(1) コンピュータ，コンピュータ・システム若しくはコンピュータ・ネットワークに，故意かつ無権限でアクセスし，若しくはアクセスさせた者，又は，コンピュータ・システム・サービスが全面的に若しくは部分的に，他人により所有され，他人と契約され，若しくは，他人に対して，他人のために，若しくは他人と連結して運営されている場合に，当該コンピュータ・システム・サービスの利用権限の与えられている利用者に対するコンピュータ・システム・サービスを故意かつ無権限で拒否し若しくは拒否させた者は，コンピュータ利用者に対する罪を犯したものとする。

(2)(a) 本項に別に定めるところのほか，コンピュータ利用者に対する罪は，第 775.082条，第 775.083条又は第 775.084条に定めるところに従い処罰される，第３級の重罪となる。

(b) それが財産を騙取し，又は収得するための計画又は策略を企て，又は実行するために犯された場合は，第 775.082条，第 775.083条又は第 775.084条に定めるところに従い処罰される，第２級の重罪となる。

（本章の非排他性）

第 815.07 条

本章の各規定は，本章に違反する行為に対して現在適用され，又は将来適用される当州刑法の他の規定の適用を排除するものと解釈してはならない。ただし，その規定が本章の条項に抵触する場合はこの限り

でない。

（※１）第３級の重罪は，５年以下の拘禁（§ 775.082）及び５，０００ドル以下の罰金（§ 775.083），再犯の場合は１０年以下の拘禁（§ 775.084）である。

（※２）第２級の重罪は，１５年以下の拘禁（§ 775.082）及び１万ドル以下の罰金（§ 775.083），再犯の場合は３０年以下の拘禁（§ 775.084）である。

（※３）第１級の軽罪は，１年以下の拘禁（§ 775.082）及び１，０００ドル以下の罰金（§ 775.083）である。

カナダ刑法（１９８４年改正）

３０１．２条

(1) 詐欺的にかつ権限なく

(a)直接若しくは間接にコンピュータ・サービスを取得し、

(b)電磁的、音響的、機械的若しくはその他の手段により、直接若しくは間接に、コンピュータのなんらかの作用を傍受し若しくは傍受を受けしめ、又は

(c) (a)項、(b)項に規定する犯罪若しくはデータ若しくはコンピュータ・システムに関連して３８７条に規定する犯罪を犯す目的で、直接若しくは間接に、コンピュータ・システムを利用し

た者は、正式起訴犯罪として１０年以下の拘禁刑に処し、又は、略式手続犯罪として処罰する。

(2) 本条において、

「コンピュータ・プログラム」とは、コンピュータ・システム内で実行された場合に、コンピュータ・システムをしてある作用を遂行させるに至る、命令又は陳述を意味するデータを意味し、

「コンピュータ・サービス」は、データ処理及びデータ記憶若しくは検索を含み、

「コンピュータ・システム」とは、

(a)コンピュータ・プログラム又はその他のデータを含み、かつ

(b)コンピュータ・プログラムに従って、

（ｉ）論理（演算・・訳者注）及び制御を遂行し、かつ

（ii）その他のなんらかの作用を遂行し得る

装置又はその一部にかかる装置を含む相互接続され若しくは関連する装置のグループを意味し、

「データ」とは、コンピュータ・システム内における利用に適する形態に準備され又は準備されつつある情報又は概念の表現を意味し、

「電磁的、音響的、機械的又はその他の装置」とは、コンピュータ・システムのなんらかの作用を傍受するのに用いられ又は用いられ得るあらゆる装置又は機器を意味するが、利用者の聴覚異常を矯正するのに用いられる補聴器を含まず、

「作用」は、論理、制御、算術、削除、記憶及び検索、並びに、コンピュータ・システムとの、コンピュータ・システムからの又はコンピュータ・システム内での通信又はテレコミュニケーションを含み、

「傍受」は、コンピュータ・システムの機能の聴取若しくは録取又はこれを意味し若しくはその趣旨を含んだ物の取得を含む。

３８７条

(1.1)故意に

(a)データを破壊若しくは改変し、

(b)データを無意味、無益若しくは無効にし、

(c)データの正当な利用を妨害、中断若しくは干渉し、

(d)他人がデータを正当に利用するのを妨害、中断若しくは干渉し、又は、

アクセスの権限を有する者に対しデータへのアクセスを拒否し

た者は、損壊罪（mischief）とする。

(5) データに関して損壊罪を犯した者は、

(a)正式起訴犯罪として１０年以下の拘禁刑に処し、又は

(b)略式起訴犯罪として処罰する。

(5.1)故意に一定の作為をし又は故意に自己の義務たる作為をしなかった者は、当該作為又は不作為が生命に対し現実の危険を生じさせる損壊罪又は財産若しくはデータに関する損壊罪を構成する場合において、

(a)正式起訴犯罪として５年以下の拘禁刑に処し、又は

(b)略式起訴犯罪として処罰する。

4. その他

(1) 「電気通信事業者の取扱い中に係る通信」

(電気通信事業法§104)の範囲について

- 土屋委員（当委員会・昭和62年度レポート）

電気通信事業法第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回線に接続さ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。

- 渥美委員（当委員会・昭和62年度レポート）〔抜粋〕

電気通信事業法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。

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。

(2) 「財産的情報の刑法的保護」

—— 昭和63.7.25 当委員会での西田委員講演要旨 ——

(この講演は、昭63.5.28 に日本刑法学会において発表された「財産的

情報の刑法的保護」と題する共同研究の内容についての説明である。）

・　規定案

第一　職務上知り得た他人の財産価値を有する技術上または営業上の秘密情報を窃用（その情報の本来の用法に従って不正に利用し、それにより当該情報の有する財産価値を侵害）すること（5年以下の懲役または罰金）。

第二　職務上知り得た他人の財産価値を有する技術上または営業上の秘密情報を窃用の目的で漏示すること（3年以下の懲役または罰金）。

第三　他人の財産価値を有する技術上または営業上の秘密情報を窃用の目的で不正に取得すること（3年以下の懲役または罰金）。

・　講演要旨

ここでの論点は、財産的価値を有する情報に対する刑法的保護の必要性である。これを次の三つの規定案として考えた。即ち、1　職務上知りえた他人の財産的価値を有する情報を窃用すること、2　同情報を窃用の目的で漏示すること、3　他人の財産的価値を有する情報を窃用の目的で不正に取得することの3点であり、これらを刑法の財産犯の類型として導入すべきであるということである。

その理由として、財産的価値を有する情報の侵害が世の中に相当数現れてきており、財産的情報の犯罪に対し、既存の財産犯に対する規定によって対応している判例があることが指摘できる。そして、既存の刑法の財産犯的規定においては、構成要件の立て方がうまく出来ていないのではないかと考えられる。

現行法上の対応の問題としては、有体物というものを基本とした財物移転罪としての窃盗あるいは横領といった規定が、情報的財産に拡張ないしは転用して用いられているという点がある。例えば、情報の窃取を

コピー用紙の窃盗におきかえている例がある。また、使用窃盗ないしは一時無断使用による原本ではなく情報のコピーをとることについても、下級審等では不法領得の意思を認めてきている。

有形物に化体された無形的情報を刑法 235条の財物の中に含めて、あるいは拡張して処罰してゆこうという方向が判例の中でも色濃くでてきている。しかし、このような判例の方向は財産犯規定のあり方としては健全なものとは言い得ないものであり、財物移転罪という刑法 235条窃盗罪は、有体物の占有によってその権利者が有している具体的利用可能性が保護の対象になっているのである。

これに対して、情報においては、それが窃取されてもそれ自体はなくならないので、利用可能性は侵害されない。この場合は普通の窃盗罪と違う性質を持っている。情報の窃取に窃盗罪で対応することは無理があり、解釈論としても正当ではない。

情報の窃取は、情報が拡散したにすぎないのであって、そこでの侵害の実体は、情報を独占的に利用しうる地位という経済的権利が侵害されたということにほかならない。情報侵害罪は財物移転罪とは違って、独占的に利用しうる情報の権利が侵害されることによっておきる経済的不利益に対応するのである。

情報のもつ特殊な性質と現行法における財物移転罪の相違点を考慮すれば、新たな立法によって対処すべきであるという結論が導かれる。そして、通信回線に侵入して情報を盗み出すというような財物性を超えた場合の窃盗罪では対処できないような事態に対して新たな立法ということを想定せざるを得ない。

これらを基礎に立法を考えた場合、不正競争防止法の中に、情報侵害の罪を新設するという考え方があるが、我々は不正競争防止法に入れることは考えない。なぜならば、第一に、不正競争防止法は公正な競争秩序を守るという意味からその目的は社会的法益にならざるをえない。

財産的情報を刑法的に保護するという場合、その保護の対象は財産的利益である。第二に、不正競争防止法に財産的価値を入れたドイツにあっては、競業的目的の外に図利目的、加害目的、第三者のためにという目的まで入れてしまったために、目的による制限と言うものが意味をなさなくなってしまった。財産の一つの存在形態としての情報の保護、とくに東側諸国を意識した西ドイツの国家的保護という意味になっている。

第三に、不正競争防止法にとりこんだ時に、現在の罪の形にどれほどのインパクトを与えられるか、現在の不正競争防止法でも最高で3年の刑であるが、情報、資料の一時持出しでも窃盗罪に当たるので、刑期を変えることにはならず、刑法 235条で処罰できない無形的侵害対応について、不正競争防止法で補完する役割しかもたない。

第四として、コンピュータ・データの不正取得罪を新たに設けると言う考え方で、西ドイツ刑法の 202条A項がこれを規定している。コンピュータ・データの不正取得罪というものは、侵害の客体としてのデータが極めて明らかに限定できるというところに、ポイントがある。

コンピュータ犯罪とも関連して、わが国でも、コンピュータ・データの不正取得という罪が設けられることが十分考えられるが、我々の研究グループはこの点も取り上げなかった。なぜならというに、第一に、コンピュータ・データであるというだけで保護する必要性があるとは認められないからであり、また、国家機密、プライバシー・データもこの中に含まれ、定義が曖昧になってしまうからである。そしてこのように実施したとしても、磁気テープやフロッピ・ディスクの持出しが窃盗罪を構成するので、実務の形態は変わらないと考えられる。

このようにして、我々の研究グループとしては、財産犯として構成すべきであるという結論に至った。この場合にも、財産犯の客体としての情報を考えた場合に、市場価値を形成しうる財産価値としての情報、あるいは交換価値を有するものであれば全てこれにとりこむべきであると

いう考え方の、情報財というものとして把えるやり方、これはわりあいなじみやすいやり方ではあるが、これもここでは採用しない。

即ち、交換価値を有する情報を全て保護するとすると、これは加害者にとって交換価値を持てば良いということであり、そして、加害者がこの情報をお金に換えることができれば良いということが要件となるが、このように言ってしまうと全ての情報が交換価値を持つ、お金に換えることができると言えるようになり、この考え方は情報侵害、機密侵害全体をカバーすることになってしまう。そこで我々のグループとしては、加害者が財産的利得を得られると同時に、被害者が財産的損害を同時に受けるという要件をもうけるという結論に至った。

例えば外交的機密など、国家機密は加害者がこれを売って利得を得たとしても、国家は財産的損失を蒙ったとは言えない、またプライバシー・データについても人格的の侵害にはなるが、財産的損失とはならないので、財産犯には該当しない。

加害者と被害者双方の財産的価値を特定することによって、客体としての情報が明確に限定され、顧客情報についても競争企業間で窃用されれば財産犯の対象となるが、非競争企業との間では処罰の対象とならない。この場合被害企業には、顧客情報の開発コストの逸失が考えられるが、これは財産犯ではなく、著作権、知的所有権の対象になると考えられる。

このような方法によって、我々の立論は侵害の実体としての情報の範囲を明確に限定できるのではないかと考える。この考えは、処罰すべきものも除外してしまうという意見もありうるが、一般的情報犯と一線を画するという意味がある。次に、財産犯を刑法典におくことにより、財産犯を従来の窃盗罪と区別することに意義がある。原本の実物の一部を盗んだという場合に、これが窃盗罪に当たるか財産犯に当たるかということに議論があるが、この場合も窃盗罪ではなく財産犯に該当する扱い

としている。

これと同時に、磁気テープやフロッピ・ディスクのようなものの媒体自体の価値も認めるべきであるという議論がでてきているが、これはさほど本質的な議論ではないと考えている。

これに対し、法益侵害の形態として窃用があり、その予備的行為として情報の探知や漏示という行為がある。窃用の法定刑は5年、探知・漏示については3年と、現在の10年という窃盗罪の刑よりはるかに軽い刑を考えている。その理由は、情報の非移転性という意味から情報の元はなくならないという点を考慮したものである。

これらをまとめると、窃用という基本類型のもとに立法の必要性を認め、探知と漏示がこれを前提としての危険犯となる。情報の非移転性それから全体財産に対する危険性を考慮して、現行の窃盗罪よりはこれを低くする。そして客体としての財産的情報は、加害者が財産的利得を得ると同時に被害者が財産的損失を蒙むるという要件をおくことによってこれを限定する。そしてこのような不正な財産犯を一つの類型として刑法典に盛り込むことによって、現在財物移転罪を中心として構成されている既存の財産犯規定を情報に適用することによって生じている様々な不合理、適切でない面を、立法によって修正したいということである。

(3) ＯＥＣＤコンピュータ関連犯罪特別委員会報告

「コンピュータ関連犯罪　ＯＥＣＤ地域における法的政策の分析」
（ＤＳＴＩ／ＩＣＣＰ／84.22 第１改定版　Scale Ｅの抜粋）

（編注）

この報告は、事務局が加盟国に対して行った「コンピータ犯罪の抑制に関する質問」への「分析的要約」として作成されたものである。その目的はコンピータ関連犯罪への対応に関して、a)加盟国の情報交換を容易にし、b)加盟国がとる手段の展開と傾向を観察記述し、C)犯罪と法律についての共通の理解に到達するためである（報告序論）。

第３章　実体刑事法の分析および法的政策への提言（1985.8.30 起草）

2　コンピュータ・スパイおよびプログラム盗用

146.　コンピュータ・スパイおよびプログラム盗用に刑法や民法を如何に適用するかは、今日のコンピュータ犯罪の分野での最大の主題であり、経済的に重要な法的問題に入るものである。体系的な法的アプローチは、(a)コンピュータ記憶データすべて（データ・ベースおよびコンピュータ・プログラムを含む）の一般的保護か(b)コンピュータ・プログラムの追加的保護を区別するべきである、とする。

a）　コンピュータ・システムの一般的データの保護

aa）伝統的財産法

147.　他人に属する有形の情報を運ぶもの（例えば紙のリスト、テープ、

ディスク）を取り去ることによって情報を得た場合に、西側諸国の法体系すべてにおいては、盗み、窃盗、横領の伝統的な規定は何ら特別の問題を生じない。しかしながら、データ処理や伝達システムがデータを速く、人目につかないで、多くの場合遠距離通信設備によって、コピーできることから、これらの伝統的「情報を運ぶものの窃盗」のほとんどが、情報をデータ装置にコピーする行為に取り代わった。従って、どの範囲にまで無形の情報の純粋取得にこれらの規定が及ぶかの問題が生じる。

148. ドイツやイタリーのような大陸法の国のほとんどにおいては、窃盗や横領に関する伝統的な規定を、情報の許されざる抜き取りに適用したがらない。何故ならば、これらの法律は一般的に、被害者から永久的に奪う故意をもって、有形財産を取ることを要件とするからである。（例えば、ドイツ刑法 242条、246 条を参照）。

149. しかしながら、一部の大陸法の国においても、窃盗や横領に関する伝統的な規定を、少なくとも有形のデータを運ぶものを一定の間犯罪者が所持する場合には適用できるようである。このことは、例えばフランスに妥当する。フランスでは、1979年 1 月 8 日の判決によって最高裁判所刑事部が文書のフォトコピー行為を窃盗罪として刑法 379条により判断した。しかしながら、フランスの学説は、この判決を情報窃盗の一般的概念に拡張することに反対である。オランダではアーンハム上訴裁判所は1983年10月27日の判決において更に進んでデータはオランダ刑法 321条にいう「品物」を表わすとみなした。その裁判所は自分自身のビジネスを設立する目的でコンピュータ・プログラムをコピーした従業員を横領罪で有罪と宣言した。同様の結果は窃盗に関する法律が電気に適用されている国においても得られるであろう。例えば、ギリシャにおいては、エネルギーは刑法 372条にいう「物」と考えられ、フィンランドでは1950年最高

裁判所が電力は窃盗の規定にいう「品物または金銭」を構成すると類推によって判決した。しかしながら、情報はエネルギーの別の形にすぎず、同じ原則を両方の「無形物」に適用できるという考え方は、全く問題である。何故ならば、エネルギー窃盗の場合には、エネルギーは取り去られてしまうのに対して、情報の権限なき取得の場合には情報は所持者のもとにとどまっているからである。

150. 英国において、長期間にわたって窃盗に関する法律を電気に適用してきたが（1916年の窃盗法およびビクトリア朝時代の窃盗法をも参照）1968年の窃盗法は「財産」には次のものを含むと定義する。それらは「金銭もしくは他のすべての財産、動産不動産、債権および無形財産を含む」。しかしながら、イギリス法は単に伝統的窃盗規定の対象を拡張することは、知的財産窃盗を包含するのに十分ではないことを実証している。それは「永久的に他人からそれを奪う」故意を要件とする特定の条文は、今でも有形物について言うようであるからである。Oxford vs. Moss 事件においてイギリス控訴裁判所は1979年に、機密情報（例えば、学生が不正に取得した大学の試験問題）は1968年窃盗法4条にいう無形財産に入るものではないと判決した。

151. 知的価値を「財産とする理論」への強い傾向がアメリカの判例に認められる。アメリカでは特定の条件で1964年企業秘密の窃盗に対して刑事罰を探しはじめた。アメリカの一部の州裁判所はコンピュータ・データを伝統的窃盗規定にいう財産と見なしている。その他の州の多くでは、州政府がコンピュータ・データまたは企業秘密を「財産」または「価値ある物」と定義し、窃盗規定またはコンピュータ犯罪に関する新しい一般規定が適用できるようにした。しかしながら、窃盗に関する規定を拡張して情報に及ぼすことにも問題が生じる。Hancock vs. State 事件と対照的に、これはプログラムの

「窃盗」が肯定された事件であるが、Ward vs. Superior Court of California事件では、コンピュータの記憶に入っているプログラムの窃盗は、関連制定法の内容である犯罪の定義の範囲に属す「品物」の「窃盗」と見なすことができないと判示した。People vs. Home Insurance Company 事件において、コロラド州の裁判所もまたコンピュータのインパルス（機密の病院記録に関する）をそれぞれの制定法の意味に含まれる有形財産と見なすことができないとした。（この制定法は後に一般的コンピュータ犯罪法の中で財産を広範囲に定義して修正された）。the United States vs. Seidlitz事件で、コンピュータ・ソフトウェアが遠くの端末を使ってコピーされた事件においては、盗品の州際輸送の罪を適用しようとしたが法的にできないことが認定された。何故ならば、財産の「輸送」（元の場所からの移動）があったとは証明できないであろうからである。情報についての財産保護がこのように困難であることから、アメリカの多くの州は最近、一般的な窃盗規定とは別に存在する、企業秘密の窃盗とその開示に関する特別規定を制定した。フロリダ州とミズリー州のコンピュータ犯罪に対する制定法は企業秘密のため、コンピュータに特定のアプローチを例示し、データが形成する企業秘密の開示に適用される特別規定を含んでいる。

152. カナダの判例は最近アメリカの進展状態に続いているようであるが、最終的な問題解決には至っていない。労働組合のメンバーがホテル従業員の住所の入っている極秘の従業員名簿のプリント・アウトをコピーしようとした Regina vs. Stewart 事件において、高等裁判所は第一審において、損壊、詐欺、窃盗に対する起訴を棄却し、秘密情報は窃盗に関する法律にいう財産ではないと判決した（カナダ刑法 283条）。しかしながら、オンタリオ州控訴裁判所は、判決を覆えして窃盗教唆の罪で有罪とした。無条件釈放が認められたけ

れども、犯罪者は現在カナダ最高裁判所に自分の有罪を争って上告し、ここ数ヵ月でその問題の最高裁判決が下されることになっている。カナダの「正義と法律問題に関する常任委員会」のコンピュータ犯罪に関する小委員会は、改正の討論中にこの問題を考察し、現在財産的アプローチに反対することを決め、議会が情報に財産価値を認めることによって情報を保護しようとするのは思慮が足りないことだろうと述べた。

153. この勧告に対して、オーストラリアのコンピュータ・ソフトウェアおよび情報を含む「コンピュータ関連財産の窃盗」に関する改正案は、財産のアプローチに基いている。

154. 有形財産と知的価値との相違（財産は排他性の意味を含み、一方情報は一個人では完全に「補える」ことのできない公益性がより大きい）、伝統的財産権と知的財産権の相違（例えば、所有権と占有の問題に関して）、伝統的な有形物の窃盗と情報窃盗の相違（そこでは問題となっている情報はコピーされたにすぎず所有者の手許にとどまっている）のために、財産の理論は知的価値の一般的保護のために否定されるべきである。民事法は情報それ自体を保護できるとは見ていないし、著作権、特許権、商標権、工業意匠権は制定法により独占権を与えられているが、その作品の創作者、発明者、意匠図案家は一定の限度内での専有権を与えられるにすぎない（特に時間と地理的領域においては）ことを忘れてはならない。従って、民事法が扱ってさえいない価値を刑法によって保護することは危険でありかつ不必要に思われる。その上、刑法に関する限りでは、情報を「取る」とか「被害者から奪う」とかについて言うことは言葉をねじまげることが多い。同様の主張はまた犯罪によって取得した財産の所持に関する規定や盗品の受取りに関する規定の適用を不可とする（例えば、カナダ刑法 312条、ドイツ刑法 257条を参照）。

少なくとも大陸法系の国の観点からは、窃盗規定や盗みの規定から独立した解決策が好ましいことは疑いの余地がない。

bb）企業秘密および不当競争法

現在の法的状況

155. 一般的な財産法を企業秘密に適用することは大抵の大陸法の国においては問題があるので、他人のデータの不正流用または秘密情報の抜取りは企業秘密の漏示または不正流用を禁ずる特別規定によって網羅する。これらの規定は、一定の罰すべき情報取得行為を刑法規定または不当競争禁止法の刑事もしくは民事の規定のいずれかによって禁じて、企業秘密を保護するものである。この企業秘密保護および公正競争の概念は、現代アメリカの情報理論と調和する。この理論は静止状態の「財産理論」を退け、手続的「関係理論」や「権利を与える理論」へと、開示者と被開示者間の関係に着目しつつ、動いている。

156. コンピュータ・データやコンピュータ・プログラムの秘密が保たれている限り、企業秘密法の刑法規定は漏示者や不正直な行動をした者に対する効果的な武器となり得る。ドイツにおいては、雇用中の従業員または「善良なる風俗に反する」者によって企業秘密が開示されまたは使用された場合、効力のある刑法上、民事上の保護が与えられる。特に不当競争禁止法の17条、18条、20条において、不正使用されたプログラムがひどく改変された場合でさえも、大抵の大陸法系の国においては、法的状況は同様で、例えば、スイス不当競争禁止法13条、スイス刑法 162条、273 条、またはオーストリア不当競争禁止法11条、12条、19条に例示される。しかしながら、企

業秘密規定が一部しか十分でない国もある。例えばフランスの制定法は産業上の企業秘密に限られ（フランス刑法 418条）、ルクセンブルグ法（刑法 309条）で、ベルギーおよびイタリー法には外部の人間によるスパイ行為には弱い抜け穴がある。オランダは例外で特別の企業秘密法を持たない。

157. しかしながら、これらの大陸法系の国々のほとんどでは産業スパイを禁ずる刑法規定をもっと広範囲の民事規定が支援している。例えば、ドイツ不当競争禁止法１条は、丸うつしの模倣や寄生的競争に対して民事上の保護を追加して与える。同様の結果は、ベルギーの1971年７月14日の公正企業行為法54条、イタリア民法2598条、フランス民法1382条、1383条および「不当競争」、「干渉行為」、「他人の知的労作を不当に利用しての不当利得」についての関連理論、またはオランダの不当競争の一般的概念からも生じる。

158. アメリカにおいては、企業秘密法および不当競争法は一般的に州法であって、大部分は制定法ではない。しかしながら、前述の如く、州によっては企業秘密の不当な開示またはその窃盗に関する刑法を制定しているし、多くの州がコンピュータ犯罪（データおよびプログラムの窃盗を含む）を禁ずる特別規定を提案した。その上、統一州法委員全国会議は1980年に「統一企業秘密法」を勧告し、その後それが採択されたのは、例えば、アーカンソー、デラウェア、アイダホ、インディアナ、カンザス、ルイジアナ、ミネソタ、ノース・カロライナ、ワシントンである。英国の裁判所がとる狭く、かつ慎重な見解に反して、アメリカの裁判官は不当競争を非常に広義の訴訟原因とした。それは連邦先占の法理によってのみ制限される（特に連邦の商標法および著作権法に関して）、コンピュータ・プログラムの企業秘密保護を考察して、アメリカの裁判所は、商業用のプログラムを何百何千もの受領者に広く配布することはその基礎とな

っているプログラムの企業秘密の地位を失わせるものではない、と認定した。但しライセンス契約が受領者一人一人にプログラムの使用と開示に関して制約をしている場合を条件とする。

159. カナダ刑法もまた企業秘密の開示を犯罪と認めない。刑法上の保護は委任に関する規定および刑法上の背任の規定のもとでのみ求めることができる。企業秘密の不法流用と主張されるものの民事訴訟手続きは、信託関係、信託違反、不当利得の法理の事件に対して、契約法または衡平法に依拠しなければならない。このことは両当事者間に明確な信任関係がある場合に非常にうまく機能する。しかしながら、保護は企業秘密が第三者に伝えられた時には不確実なものとなる。

160. 英国は企業秘密保護の領域で特別の刑事立法はない。一定の事件では信頼違反の争点のみが適用される。

161. 日本においてもまた権限なくして企業秘密を開示し、またはそれにアクセスすることが明示的に入った刑法規定その他の制定法はない。民事上の企業秘密保護もよく発達しておらず、一般的な不法行為規定または契約法のもとで求めなければならない。

改訂案

162. 刑事、民事上の企業秘密保護の改正案は諸国で作成された。ドイツにおいては、現在討論されている不当競争禁止法の修正は、一定の定義された技術的手段による企業秘密の使用のみならずその取得も罰することを提案している。スェーデンの企業秘密保護に関する委員会が提言するのは、1931年の不当競争禁止法の企業秘密に関する条文を産業スパイ、商売上の関係または使用者と従業員の関係での商売上の秘密の濫用を区別する新制立法によって拡張することで

ある。フィンランドでの刑法改正特別調査委員会の改正案は、企業秘密が不法に開示され、または利用された場合に、データ処理システムまたはデータ伝達ネットワークへの許されざる侵入等によって、他人の企業秘密へのアクセスを得ることを犯罪とすると提言した。

163. カナダでも、企業秘密保護法は連邦と州の共同委員会が準備中である。英国においては法律改正審議会は最近新しい制定法上の不法行為の創設をめぐる立法計画を勧告した。アメリカでは民事上の企業秘密保護の領域で前述の統一企業秘密法のモデルが支持された。しかしながら、刑法の領域では、改正はあらゆるコンピュータ記憶データの不法取得を含むコンピュータ犯罪を禁ずる一般的規定の確立に基いている（前出を参照）。

164. 日本においては、早くも1974年に1974年改正刑法草案 318条が提案された。

法的政策の評価と提言

165. 将来の政策決定に関する限り、国際的に企業秘密保護に向う傾向は助長されるべきである。企業秘密保護は単に財産への自然権に基くばかりでなく、主として一定の目的として法律によって促進、規制されるべきだという確信に基くものである。そのような保護がある程度なければ、調査研究やその費用は危険にさらされるであろう。

166. しかしながら、情報の独占を避けるために、企業秘密保護は情報取得の一定の我慢できない行為に制限すべきであって、情報そのものの保護にまで及ぶべきではない。従って、情報の許されざる複製をする犯罪を、もっと広く解釈することは望ましくなく、調和がよくとれた伝統的著作権体系を損なうであろう。

167. 著作権体系がコンピュータ・プログラムに適用される限り、企業

秘密法の価値は、この領域で著作権法の適用があるために廃用されるのではない。何故ならば、企業秘密法はアイディア、情報、新しいものを保護することができ、従って、著作権法によって保護されない要素を網羅するからである。他方、著作権法の価値は廃れるわけではない。何故ならば企業秘密は秘密でないプログラムの領域には適用がないからである。その上、企業秘密法は一般的に善意でその秘密を取得するであろう第三者に対しては用いることができないのである。（例えば、犯罪者から不法取得したデータを買うなど）。

168. 企業秘密法の分野における刑法草案を作成するにあたり、情報交換の多様なレベルを区別するべきである。特に国内および国際的情報交換、商業上の関係での情報交換、使用者と従業員の関係での情報交換の分野においては。国際的情報交換は企業秘密法の政治的次元を示している。工業国は自国で開発した工程のあるものの、他国による盗用の予防に関心をもつ一方、特に発展途上国はそれらの法律が「持つ」国と「持たざる」国の間の情報と技術の自由な流れを妨害するであろうから、そのような法律には猛烈に抵抗する。企業の内部、外部の情報交換に関しては、労働者の移動性に特別な注意を払いつつ、雇用者と従業員の利害の均衡に特に注目すべきである。従業員は雇用中に私的利益を得るために雇用者の企業秘密の利用を許されるべきではないが、雇用期間終了後も少くとも自らの仕事の経験を保持する権利を与えられるべきである。従って企業秘密保護は、犯罪者の地位によって資格を与えられるし、依拠するのである。

169. 国際的コンセンサスに達するためには、次のことが勧告できるであろう。すなわち、ＯＥＣＤ加盟国すべての法体系…… 刑法または不当競争禁止法のいずれでも ……か不当競争に関する適切な民事法規定が支援する刑法上の企業秘密保護を確立することである。これらの刑法、民事上の規定は、一般的にすべての企業秘密（所有

者が企業秘密として取扱うもの）に適用されるべきであって、コンピュータやデータ処理の分野に限られるべきではない。使用者と従業員の関係を特別に規制することは必要である。企業秘密規定は、新しいフィンランドの提案のいくつかが示唆するように、企業秘密が開示あるいは利用された場合ばかりでなく、純然たる不法コピー行為の場合にも適用できるべきである。情報技術が情報の不正流用の次元ばかりか技術をも拡張したので、これらの手段も…… フィンランドの法案が示すように…… また、例えばデータ処理システムへの不法なアクセスといったコンピュータへの特定の攻撃をも包含する。

cc）特別な秘密と関係の保護

特別な形の情報の保護

170. 特別な秘密と特別な型の情報に関してはもっと広範囲にわたる刑法上の保護が既に存在する。例えば、高度の慎重を要する軍事、技術、外交情報はすべての国においての反逆罪や一定技術の不法輸出の規定により保護されている。反逆罪の規定には一般的にコンピュータの特定の問題が示されていないし、コンピュータ記憶情報の狭い分野にのみ適用できるので、ここでは詳しく取扱わない。しかしながら、輸出規制に関して、合衆国国防省は最近コンピュータの輸出をより厳しくし、輸出監督法によってアメリカからの輸出が検閲を受けねばならない高度技術のリストにソフトウェアを含めることを要求した。この問題は現在パリで、多国間輸出調整委員会（cocom)により考察されている。

171. もう一つの特殊な型の情報の特別な保護の例は、プライバシー保

護規定、特に多様なデータ保護法案である。プライバシー保護の特別法がオーストラリア、オーストリア、カナダ、デンマーク、フランス、ドイツ、イタリー、ルクセンブルグ、ニュー・ジーランド、ノルウェー、スペイン、スエーデン、英国、アメリカでは制定され、ベルギー、フィンランド、ギリシャ、オランダ、ポルトガル、スペイン、スイスでは計画されている。国際的レベルでは、プライバシー保護および個人データの国境を越えるデータの流れを管理するＯＥＣＤの指針（1980年）、および個人データのコンピュータ処理に関する個人保護のためのヨーロッパ会議国際協定（1981年）がこれらの法律により入れられるべき原則を確立した。以上説明したごとく、この問題は詳しく取扱うべきではない。何故ならばこれら前述の手段はこの特定の領域における共通の基準を確立したからである。

特別な法律関係の保護

172. 秘密の特定的保護はまた特別な関係……例えば国家公務員と一定の従業員の仕事……にも適用がある。そこでは公務員、遠距離通信、郵便での従業員、特別な職業につく者による情報の開示に対して刑法が保護を補足、加重している。（例えば、カナダでは刑法 383条の秘密委員会委員の犯罪；ドイツ刑法 203条、204 条、3536条、354 条、355 条；スイス刑法 320条、321 条、イギリス1969年郵便法６条；アメリカ18 U.S.C. 1902～1980、 15 U.S.C. 552 (b)(1)(1976)）、一部の国では許されざる開示に対する情報保護もまた刑法の背任に関する規定から生じている（カナダ刑法 296条、ドイツ刑法 266条、日本刑法 247条）または「背任罪」（フランス刑法 408条）。特別な場合には汚職に関する規定もまた適用される（例えば、

ドイツ不当競争禁止法12条およびドイツ刑法 331条、334 条、フランス刑法177 条から 179条を参照）。これらの規定は特定的にデータ処理の分野を目的としていないので、ここでは分析しない。

173. しかし、職業上の秘密を保護する刑法規定をコンピュータに特定して拡張することは注目に値し述べる価値がある。それは一部の国で開発中であって、フランス刑法改正審議会は現在職業上の秘密（刑法 378条）を一般的な「秘密の情報」に拡張することを討議中である。論議中の規定は秘密の医療上の情報（刑法 378条）に関する法的要件を保護する規定を類推して構成し、データ処理の領域で働く人に委ねられた情報をも網羅しようとする。ポルトガルのデータ保護法案もデータ処理の分野における職業上の秘密の侵害の概念に基づく規定を含む（38条、39条、40条）。フィンランドでは刑法改正特別調査委員会は遠距離通信秘密違反に関するより特定的な規定を論議中である。職業上の秘密保護の規定は、特に職業上の秘密の保証に行き届いた伝統をもつ国においては、非常に注意深く検討されるべきである（例えば、イタリア刑法 662条「職業上の秘密」の一般的保護を見よ）。しかしながら、データ処理の分野での秘密情報は大部分企業秘密保護、プライバシー法、伝統的職業上の秘密で網羅されていることも考えねばならない。その上、データ処理の領域で働く人の定義や限界は、特にパーソナル・コンピュータが広く用いられることにかんがみ、非常に困難であり、職業上の秘密侵害に関する規定はＯＥＣＤ加盟国でかなり異なっている。従って、そのような制定法がすべての国に適当であるかどうかは疑わしい。

b) コンピュータ・プログラムの保護の拡大

174. すでに論じた法的構造、特に企業秘密法および契約法はコンピュ

ータ記憶データすべてに適用があるばかりでなく、コンピュータ・プログラム保護の重要な手段となる。しかしながら、これらの法体系は秘密のプログラム、特別関係および／または情報へアクセスする特定的行為に限定されているので、コンピュータ・プログラムを伴う、公正で問題のない取引を保証することはできない。前述のコンピュータ・プログラムとその複製の費用の相違を考えると、コンピュータ・プログラムの取引には適当な保護体系が、秘密でないプログラム（これは特に大量販売されるプログラムにとって重要である）およびあらゆる種類の権限なき複製を網羅し、第三者に適用されるべきである。

175. 全ＯＥＣＤ加盟国では、そのような保護の拡大が、特に特許権法、著作権法、コンピュータ・プログラムの特別保護構造で、求められている。

176. 少数のプログラムしか技術的発明を含んでいないために、特許権法はコンピュータ・プログラム保護を与えることができない。そこで最近著作権保護が注目の的となっている。著作権法を適用することによる問題が今や論議の焦点となっている。（以下　略）

（注）本章は U. Sieber 氏の起草による。

結　　論

1. DSTI/ICCP/84.22 （第1版）報告の作成過程において、2ケ年にわたり、メンバー国のコンピュータ関連犯罪分野に関する情報交換を行った。メンバー国はこの作業が実り豊かなものであったと考えている。メンバー国の内のいくつかにより、作成作業の間に新たな国家的規制が作られていることが報告された。この作業によって、メンバーの殆ど全ての国の立法議会と政府委員会及び裁判所が、全ての国が同じ性格を持つ新しい種類の犯罪に直面しており、それ故同じ対策が要請されていることが浮かび上がった。その上、国際通信網の利用により、この犯罪が国際的であることが立証された。越境データ流通（ＴＤＦ）の利用の調和ある展開は、メンバー国によってこの犯罪に対する整合性ある規制が行われた場合にのみ起こり得るように見受けられた。コンピュータ避難所は作られないであろうし、外国から入って来るそのような犯罪による被害国は、ＴＤＦに否定的影響を与える可能性のある対策はとらないであろう。

2. この報告はコンピュータ濫用の量に関する既存の経験的研究を手短に記述した後に、そのような濫用は現実にあるが、現在に至るまで、その経済的重要性を国内的、国際的に評価することは非常に難しいと明確に述べている。この困難さはコンピュータ犯罪の正確な定義がないことに起因する。国際的レベルにおけるこの現象を較べられるように分析するためには、この考え方について合意に達することが必要であろう。

3. 規制の準備作業の分析やＯＥＣＤメンバー国での規制に関する作業により、コンピュータ犯罪分野におけるそのような作業が急速に増大していることが判明した。ほとんど全てのメンバー国において、このような作業が完了また

は実行中であることを特筆することは重要である。これまで行ったように、メンバー国間の情報の交流が今後とも続行すれば、それは有用であろう。

4. そのような作業の進捗とコンピュータ関連犯罪分野の国立裁判所の判決が、そのような交換において取り扱われれば有用であろう。例えばメンバー国は、事務局へコンピュータ犯罪に関する議案や法令、各国へ配布可能な国立裁判所の重要な判決を送付することができる。

5. メンバー国における規制や犯罪条項の改訂の深い分析によって、「コンピュータ犯罪」として考慮されるべき5種類の行動が定義され、コンピュータ犯罪に関する議案や法令において処罰対象に含まれ得る。

それらは、以下の通りである。

a) 資金の不法な移転を行う意思をもってなされたコンピュータ・データ and/or コンピュータ・プログラムの入力、変更、消去。

b) 偽造を行う意思をもってなされたデータ and/or コンピュータ・プログラムの入力、変更、消去。

c) 正常に作動しているコンピュータ and/or 通信システムを妨害する意思をもってなされたデータ and/or コンピュータ・プログラムの入力、変更、消去。

d) 故意に行うコンピュータ・プログラムの不法コピーの売買。

e) セキュリティ対策を侵害し、コンピュータ and/or 通信システムの責任者の授権なしに故意に行うコンピュータ and/or 通信システムへのアクセス。

これらの五つの行動は、直接間接に全ての新しく計画中又は既存の規制によってカバーされ、メンバー国によって対策が講じられる行動の「公約数」と呼びうるものを構成しているように見受けられる。

6. しかし、いくつかの問題は解決されていない。民法での取扱いがよく認識されていない「所有物」への損害を与えることを処罰する前に、民法上での問題の解決をそのような国では好んでいる。それ故、情報やデータに損害を与える行為を上のリストに含めることは不可能である。したがって、情報保護のルールはある国では民事であり、他の国では刑事である。それらは（コピーライト、プライバシー保護、秘密保護において）異なっており、それらの文脈の外で分析することは困難であるということで特殊化されている。しかしながら、プライバシーや個人情報の保護法に含まれている時は、現在の刑法罰を強化することが勧告され得るであろう。

7. そのような保護はまだ民事において明確に確立されていないことに注意するとともに、メンバー国がそのような民事的保護をどのように組織するか観察されることを勧告しうるであろう。

8. 問題は、国際的レベルにおいても未解決であり、より一層の深い研究が必要である。報告の第４章でこれらの問題のいくつかが記述されている。当面この分野の適当な国際組織及びメンバー国が、国際刑事協力に関する条約や必要あらば国際コンピュータ犯罪を含む国家規制の当否をレビューすることが勧告されるであろう。コンピュータ処理やコンピュータ化情報サービス供給の国際化に伴って、そのようなサービスの利用者と供給者は適用される国家規制について情報入手を可能にしておくことが有用であろう。この国家規制は刑事的であったり民事的であったりするので、この情報は重要である。したがって、国際的コンピュータ犯罪事件の適当な司法権を決定するために、司法権係争のための可能なルールのリストが必要である。

9. 国際刑事協力に対しては、地域性とＴＤＦの原則、及び（海外司法権のもとでの証拠の許容性、捜査と訴追のための国家間警察協力の改善の問題につ

いての）国際コンピュータ犯罪事件の国家訴追の改善に対する考慮が展開されなければならないということが、明瞭に取り残されている。

（注）「結論」は U. Sieber 氏と特別委員会事務局の共同執筆による。

参考文献資料

（本文中で引用したもの以外で、主なもの）

- 「コンピュータ犯罪と刑事立法の課題」（鼎談）大谷　実・古田佐紀・西田典之
  ジュリスト　1985.10.15
- 「情報の不正入手と刑事罰」　中山信弘　自由と正義　35巻10号(1984)
- 「新しい犯罪への対応・コンピュータ犯罪と刑法」　板倉　宏　法学セミナー 1985/10
- 「企業秘密と情報財 (1)(2)」　吉岡　一男　京大・法学論叢　117巻3.4号(1985)
- 「企業秘密の保護」　山口　厚　ジュリスト　1986.1.1 ── 15
- 「情報犯罪と刑事立法」　板倉　宏　法学セミナー　1987/1
- 「情報犯罪の規律と捜査」　渥美　東洋　ジュリスト増刊1988 "ネットワーク社会と法"
- 「コンピュータ犯罪の規律法規についての若干の国際的比較」　渥美　東洋
  法とコンピュータ　No.6 (1988)
- 「コンピュータとデータの保護」　曾根　威彦　刑法雑誌28巻4号(1988)

（外国法関係）

- 「アメリカにおけるコンピュータ犯罪処罰法」　山口　厚　ジュリスト1985.10.15
- 「西ドイツにおけるコンピュータ犯罪への対応」　井田　良　ジュリスト1985.10.15
- 「企業秘密の侵害と刑事責任－とくに西ドイツ不正競業防止法の規定に関連して－」
  佐久間　修　判例タイムズ　1985.12.1
- 「コンピュータ犯罪と1986年の西ドンツ刑法改正(1)(2)」
  クラウス・ティーデマン、神山　敏雄（訳）　警察研究　59巻2.3号(1988)
- 「アメリカにおけるコンピュータ・データの刑罰による保護」　山口　厚
  刑法雑誌28巻4号(1988)
- 「西ドイツにおけるコンピュータ犯罪処罰規定とデータの保護」　井田　良　同　上
- 「西ドイツ刑法典におけるデータ探知罪」　園田　寿
  関西大学法学論集　37巻4号(1987.12)

平成元年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　会　振　興　会　館　内
TEL（432）9384

印刷所　山　　陽　株式会社
TEL（591）0248

資　料