研究レポート

No.243　October　2005

「秘密」の法的保護と管理義務：
情報セキュリティ法を考える第一歩として

研究顧問　　林　紘一郎

富士通総研（FRI）経済研究所

「秘密」の法的保護と管理義務：情報セキュリティ法を考える第一歩として

2005 年 10 月 1 日
林　紘一郎*

要約

2005 年 4 月 1 日からの個人情報保護法の全面施行もあって、情報セキュリティに関する意識は、かつてないほど高まっている。しかし個人情報保護は情報セキュリティの一要素に過ぎず、情報という無形の財貨一般が、法的にどのように保護されているかを網羅的に調べなければ、情報セキュリティの法体系を俯瞰したことにはならない。

そこで情報セキュリティの 3 要素の第一番に上げられ、また情報の中でも機微に触れ、法主体（国家・企業・個人）が最も守りたいと考えるであろう「秘密」を取り上げ、それが法的にどのように保護されているか、またその保護を享受するためにはどのような管理責任を果たさねばならないかを考察してみた。

その結果、現在の法体系では「秘密」は法的対象として十分に考察され保護されているとは言えず、法の不整合や欠缺が見られることが判明した。また、秘密が法的に保護されるためには、保護したいとする主体が相応の秘密管理をしていなければならないが、その程度がいかにあるべきかは、必ずしも明確になっていないことも見出された。

こうした考察を、今後情報セキュリティの他の要素である「完全性」「可用性」等にも及ぼし、さらにはデジタル情報財一般に拡張していけば、情報セキュリティ法の客体としての「情報」の保護のあり方に関する、一般原則が見出されるかも知れない。本稿は未熟だが、その第一歩を目指したものであり、林・石井[2005]の前半部分を大幅に加筆・修正したものである。

目次

＊　情報セキュリティ大学院大学副学長・教授。富士通総研研究顧問。

１.「秘密」の分類

秘密とは「一般的に知られていない（非公知）情報で、知られていないことに利益（有用性）があり、秘密として管理されている（秘密管理性）もの」と考えられる。わが国の制定法において秘密を直接定義したものはなく、営業秘密につき不正競争防止法[1] 2 条 4 項が「営業秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないもの」と定義しているのが、上記 3 要素を含み本稿の文脈に最も近い[2]。

ここで秘密は、保有する主体と、それが生産・保管・流通・消費される過程、保護の態様の 3 つの要素で分類することができる。まず主体の面から分類してみると、①国家、②法人、③個人の 3 種類が考えられる。ここで法人には種々の形態があり、営利企業と NPO 法人では自ずと一定の差が生ずることは否定できない。また法人格のない社団にとっても、秘密の管理が問題になることはある。しかし何といっても、法人の圧倒的多数は企業であるから、ここでは法人＝企業と見ておこう。

また個人は、基本的人権の享有主体としての純粋な個人の側面を有するほか、自営業者の場合には法人に近似の要素を持ち、被傭者の場合には従業員（労働者）[3]として使用者との雇用契約に服することになる。また個人は、通常消費者として、国民総支出の過半を占める経済活動上のプレーヤーであるが、同時に株式を保有することによって企業を統治する側に回ることもある。このように個人は種々の違った顔を持っているが、ここでは純粋な個人を主たる対象とし、それ以外の役割の場合には、他のプレーヤー（国家または法人）との関係性の中で論じることにしよう。

まず①国家について考えてみよう。近代市民社会において国家は、基本的人権を生来保有する国民の、負託に応えて形成されるものとされているから、その保有する情報は基本的には国民のものである[4]。そこでは情報公開が原則であって、国家の秘密は存在しないし、存在すべきでないように見える。しかし、国家が自国と自国民の安全を守り、他の国家との交渉等を行なう過程では、情報を秘匿しておくことがどうしても必要な場合がある。これらの情報は、国家機密・外交秘密・防衛秘密などと呼ばれ、一定期間保護の対象とする

---

1 「不正競争防止法」（1993 年法律第 47 号）。1994 年 5 月 1 日施行。

2 裁判例においては、最二小決 1977 年 12 月 19 日が、「国家機関が単にある事項につき形式的に秘扱いの指定をしただけでは足りず」と述べ、形式的秘密説を排し実質秘説を採っている。ただしこの事案では、対象になっている「営業庶業等所得標準率表」および「所得業種別効率表」の実質秘性の検証を十分していないのではないか、との批判がある。

3 雇用契約の一方の当事者を表す用語としては「勤労者」（憲法 28 条）や「労働者」（労働基準法 9 条、労働組合法 3 条など）が使われている。この場合、法人の役員又は代表者は含まれないので、これらを含む場合には「従業者」（個人情報保護法 21 条の場合は前者のみを含み、電気通信事業法 190 条の場合は前者・後者とも含む）が使われる。本稿ではこれらの差を理解した上でなお、一般用語としての従業員に統一する。

4 このことは、わが国憲法の精神から見ても、自明のことのように思われる。ところが、わが国著作権法にはパブリック・ドメインの明文の規定がないこともあって、政府刊行物の「○○白書」の類も、形式論理的には当該官公署に著作権が発生することになる（著作権法 13 条 2 号の反対解釈）。

べきであろう。もちろん一定期間経過後は、公表されるべきである[5]。

なお、国家が保有する情報の中には、企業や個人から預かったものが多数含まれるが、先に個人が持つ複数の役割について述べたと同様、これらはとりあえず企業や個人の情報と考えておこう。ただし、これらの情報の保有主体と帰属主体の間には、往々にして利益相反が生ずることがある。これらは詳細な検討を必要とするテーマであるが、本稿では後述する「営業秘密としての顧客情報と個人情報の相克」に代表させて論ずることにしよう。

②企業についても秘密がある。国家と同様企業も、株主はじめ多くの利害関係者（ステーク・ホルダー）の利益を代表するものであるから、とりわけ株式上場企業においては、できるだけ多くの情報を公開しなければならない。近年、企業の不祥事が多発している現状に鑑み、コンプライアンスとかコーポレート・ガバナンスの観点から、情報公開の要請が高まっているのは、当然とも言える。しかし企業は同時に、市場において多数の事業者と競争しているから、競争力の源泉であるとか交渉を優位に導くための情報は秘匿せざるを得ないし、またそれを保護していくことは、市場を十全に機能させるためにも必要である。これらは企業秘密あるいは営業秘密と呼ばれる。

③個人の情報は、これまであまり注目されてこなかったが、2005 年 4 月 1 日からの個人情報保護法[6]の完全施行を機に、ある種のフィーバーが起きている。もともと個人には、私生活をみだりに公開されない権利としてのプライバシー権があることが認められている[7]。それでは、このプライバシー権と個人情報保護法による保護とは同じものなのだろうか。今のところ基本法としての個人情報保護法の円滑な実施が行なわれた段階で、いわゆるセンシティブ情報（健康状況や財務状況のような個人の機微に触れる情報）の漏洩が深刻な事態を招来したケースは乏しいので、この問題が顕在化していない。しかし、やがてこの論点はホット・イシューになるであろう。

以上の秘密保有主体に関する分類についで、情報の生産・保管・流通・消費という過程による分類がある。ここではⓐ有体物に体化[8]された秘密と、ⓑ無体物としての秘密の 2 分類が可能であり、重要である。情報はもともと無形であるが、その内容を正しく定義し誤りなく伝えたり、長期間保存する場合には、何らかの媒体に体化させるのが便利であり一般的である。このⓐの形をとると、秘密情報はそれ自体無形でありながら、書類・CD・DVD などの有形物と一体として取り扱われる。一方ⓑの形の秘密情報は、口述伝承や電話など記録に残らない手段で伝えられる。

---

[5] 情報の公開は、国民の「知る権利」の面から主張されることが多い。それが第一義的であることに異論はないが、公開は同時に、統治する側の学習に資することにも留意しなければならない。いつまでも秘匿しておくと、後の世代が教材として生かすことができないからである。

[6] 「個人情報の保護に関する法律」（2003 年法律第 57 号）ほか関連する 4 法の総称。

[7] 「プライバシーの権利」は、わが国では珍しく実定法の具体的規定を欠いたまま、裁判によって認められてきたものである。有名な『宴のあと』事件に対する東京地裁の判決（東京地判 1964 年 9 月 28 日下民集 15 巻 9 号 2317 頁）がそれで、最高裁も「プライバシーの権利」という言葉こそ避けているものの、前科照会事件に関して同旨の判決を出している（最三小判 1981 年 4 月 14 日、民集 35 巻 3 号 620 頁、判時 1001 号 3 頁）。なお、実定法上の根拠は、憲法 13 条の「幸福追求権」に求める説が有力である。

[8] 法律用語では、後述の自衛隊法のように「化体」と言うが、ここでは一般の用法に従う。

しかし、アナログの時代まではⓐとⓑの区別は有効であったが、今日ではあらゆる情報がデジタル形式で生産・保管・流通・消費されることが多くなった。コンピュータに一時的にせよ蓄積された情報は、何らかの秘密保護手段をとっておかないと、後刻不正に再生される確率も高くなったので、秘密情報は一旦「秘密」という地位を与えられれば永久に秘密であるのではなく、「秘密として守るための不断の努力を要するもの」に変化したと考えられる。

このことは、法体系全体の中で「電磁的記録」という概念が、どの程度の比重を持っているかという点と密接に関連している。「電磁的記録」は、1977 年施行の税関手続特例法[9]以来、紙という媒体に代わる記録手段として次第に認知されるようになり、2005 年施行のいわゆるe文書法[10]に到って、官―民・民―民の取引を問わず、また民事・刑事を問わず、一般的な記録手段としての地位を占めつつある。しかし、この点を突きつめていくには本稿の紙数は足りないし、また議論が発散する惧れがあるので、別の機会に譲ることにしたい[11]。

最後の保護の態様は、理念的な部分と手続的な部分に分かれる。前者の理念的な部分については、いかにも逆説的であるが、㋐あくまでも秘匿を続けることによって守るべき秘密と、㋑公開することによって公的手段によって守られる秘密に分けられる。後者はもはや秘密ではないのだから、概念矛盾と言われればそうかも知れない。

しかし、知的財産制度とりわけ特許の例を考えてみよう。特許とは産業上有用な発明に対して、国家が一定期間独占的権利を付与することによって、社会全体の効用を高めようとする施策に他ならない（特許法 1 条ほか）。そこでは、企業内に閉じて行なわれてきた研究の成果を、誰にでも利用できるようにすることが、社会全体の利益になるし、公開を前提にして一定期間の独占権を付与することが、発明のインセンティブを高めるとの認識がある（田村[2003]）。

したがって発明家ないしは彼（彼女）の属している企業は、あくまで秘密を貫き通して営業秘密としての管理を徹底することにより利潤最大化を考えるか、特許を取得（すなわち公開）して一定期間の利潤最大化を目指すかの選択肢を持っていることになる。前者のリスクは秘密の漏洩であり、後者のリスクは後発企業が特許を迂回した新たな発明をすることである。したがってここでは、特許は秘密の一形態という理解も、あながち強弁とは言えないであろう[12]。

後者の手続的部分については、これまで法学者が議論するということはあまり無かったように思う。しかし、個人情報保護法制において、法が定める部分はごくわずかで、多く

---

[9] 「電子情報処理組織による税関手続の特例等に関する法律」（1977 年法律第 54 号）。

[10] 「民間事業者が行う書面の保存等における情報通信の技術の利用に関する法律」（2004 年法律第 149 号、いわゆるe文書通則法）と「同法の施行に伴う関係法令の整備等に関する法律」（2004 年法律第 150 号、e文書整備法）の総称。

[11] 別途「電磁的記録の法的地位」として考察予定。

[12] 同様のことは企業不祥事や、インサイダー情報漏洩の扱い方についても言えそうである。あくまで秘密としての管理を貫き通すことができれば、それはそれで立派な防衛策である。しかし後刻事実が世間に知られるようになる惧れが高ければ、早めに公開してしまった方が企業が免責される度合いが高まり、より賢明な防衛策となることもあり得る。

の手続きはガイドライン等に委ねられている。また漏洩事件が後を絶たないことから見ても、秘密の管理手続への配慮を欠いて法を論じてみても、実効性に乏しいことは明らかだろう。ここでは①保護すべき秘密情報の明確化、②秘密を知り得る者の特定、③上記①②による厳格なアクセス管理、④事故の未然防止、⑤事故発生時の対策、などが争点になろう。

以上を要するに、情報はもともと拡散しやすい性質を持っているのだから、秘密を守るには相応の管理責任を問われるということである。しかもデジタル情報が一般化した現在では、管理レベルも攻撃者の技術を上回るものでなければならない。

２．国家の秘密

そこでまず、主体別に現行法の秘密保護規定を見ていこう。まず①の国家の秘密については、第 2 次世界大戦後いわゆるスパイ行為に対する罪が削除された（旧刑法 83 条～86 条）ことからも分かるとおり、わが国には「国家機密」や「外交秘密」に関する法的規律は存在しない。

これは憲法の戦争放棄（憲法前文、同 9 条）などの理想主義を貫けば、是認される措置かも知れないが、近隣に北朝鮮などの非常識な国が存在する現実に照らせば、「平和ボケ」の誇りを免れまい。もっとも、さすがに自衛隊についてだけは 2001 年の改正で自衛隊法[13] 96 条の 2 が新設され、「防衛秘密」の概念が導入された。

（防衛秘密）

第 96 条の 2　長官は、自衛隊についての別表第 4 に掲げる事項であって、公になっていないもののうち、我が国の防衛上特に秘匿することが必要であるもの（括弧内省略）を防衛秘密として指定するものとする。

2.　前項の規定による指定は、次の各号のいずれかに掲げる方法により行わなければならない。

一　政令で定めるところにより、前項に規定する事項を記録する文書、図面若しくは物件又は当該事項を化体する物件に標記を付すこと。

二　前項に規定する事項の性質上前号の規定によることが困難である場合において、政令で定めるところにより、当該事項が同項の規定の適用を受けることとなる旨を当該事項を取り扱う者に通知すること。

3.　長官は、自衛隊法の任務遂行上特段の必要がある場合に限り、国の行政機関の職員のうち防衛に関連する職務に従事する者又は防衛庁との契約に基づき防衛秘密に係る物件の製造若しくは役務の提供を業とする者に、政令で定めるところにより、防衛秘密の取扱いの業務を行わせることができる。

[13] 「自衛隊法」（1954 年法律第 165 号）。

4. 長官は第 1 項及び第 2 項に定めるもののほか、政令で定めるところにより、第 1 項に規定する事項の保護上必要な措置を講ずるものとする。

ここで別表第 4 は、次のように対象となる防衛秘密の範囲を定めている（図表 1)。

図表 1　自衛隊法別表第 4（第 96 条の 2 関係）

1　自衛隊の運用又はこれに関する見積もり若しくは計画若しくは研究
2　防衛に関し収集した電波情報、画像情報その他の重要な情報
3　前号に掲げる情報の収集整理又はその能力
4　防衛力の整備に関する見積もり若しくは計画又は研究
5　武器、弾薬、航空機その他の防衛の用に供する物（船舶を含む。第 8 号及び第 9 号において同じ。）の種類又は数量
6　防衛の用に供する通信網の構成又は通信の方法
7　防衛の用に供する暗号
8　武器、弾薬、航空機その他の防衛の用に供する物又はこれらの物の研究開発段階のものの仕様、性能又は使用方法
9　武器、弾薬、航空機その他の防衛の用に供する物又はこれらの物の研究開発段階のものの製作、検査、修理又は試験の方法
１０　防衛の用に供する施設の計画、性能又は内部の用途（第 6 号に掲げるものを除く。）

（出所）筆者作成

これに対する罰則も強化され、防衛産業に従事する者等に対しても、守秘義務・刑事罰が科されることになった（前述の 96 条の 2 第 3 項、122 条)。自衛隊員には、後述するように国家公務員と同レベルの守秘義務があるが、防衛秘密の保持義務違反に関する 122 条の罰則を要約すれば、図表 2 のようになる。

図表 2　自衛隊法 122 条による罰則

対象・違反形態	罰則
1. 防衛秘密を取り扱うことを業務とする者がその業務により知得した防衛秘密を漏らした場合（その業務をしなくなった後も同様）	5 年以下の懲役
2. 過失により防衛秘密を漏らした場合	1 年以下の禁錮又は 3 万円以下の罰金
3. 1 項の行為の遂行を共謀、教唆又は煽動した者	3 年以下の懲役
4. 1 項の未遂罪又は 3 項の罪を犯した者のうち共謀した者が自首したときは、その刑を軽減又は免除する	
5. 1 項から 3 項までの罪の国外犯は、罰する	

（出所）筆者作成

このように、防衛秘密については制度が整ったが、それ以外の情報たとえば外交機密については、「国家機密」が特別な扱いをされていないとすれば、一般的な公務員の守秘義務として守るしかない。ところが、これらの規定において、刑は意外に軽いのである。

国家公務員法[14]の関連規定は次のとおりである。

（秘密を守る義務）

第100条　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 項以下略）

第 109 条　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。

十二　第 100 条第 1 項または第 2 項の規定に違反して秘密を漏らした者

そして驚いたことに、自衛隊法における秘密保持義務も、前述の防衛秘密に関する部分を除けば、同じレベルに設定されている。

（秘密を守る義務）

第59条　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。（第 2 項省略）

第 118 条　次の各号の 1 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 項または第 2 項の規定に違反して秘密を漏らした者

これらの規定を次項で述べる電気通信事業に従事する者の責任と対比すれば、我が国がいかに「有事」を無視し続けてきたかがわかるだろう[15]。スパイに関する罪や、その対策を定めた特別法が無いこともまた、わが国が「普通の国」ではないことを暗示している。そして、さらに進んでは、こうした業務に従事する個人の忠誠心を確保する方法（人的クリアランス）まで考えねばなるまい（永野[2004]）。

わが国で唯一、有事に備えた秘密保護規定があるとすれば、それは日米相互防衛援助協定等に伴う秘密保護法[16]により規定された、特別防衛秘密である。特別防衛秘密は、わが国がアメリカから導入する主要な装備品等（ライセンス生産、FMS調達、一般輸入による調達）のうち、次に掲げる事項およびこれら事項にかかる文書、図面又は物件で公になっていないものをいう。

---

[14] 「国家公務員法」（1947 年法律第 120 号）。

[15] もっとも、これは「国家公務員の無謬性」という神話の故とする見方も成り立つ。わが国では「お上は悪いことをしない」という神話が支配してきたからである。しかしこの神話も、相次ぐ公務員の不祥事で馬脚を現してしまった。

[16] 「日米相互防衛援助協定等に伴う秘密保護法」（1954 年法律第 166 号）。

1.　日米相互防衛援助協定等に基づき、アメリカから供与された装備品等
　イ　構造又は性能
　ロ　製作、保管又は修理に関する技術
　ハ　使用方法
　二　品目および数量
2.　日米相互防衛援助協定等に基づき、供与された情報で、装備品等に関する前号イからハに関する事項

従って、現実に装備品等が供与されていない場合でも、それらに関する情報のみが供与された場合を含むことになる。罰則は、日米相互防衛援助協定に伴う秘密保護法3条から6条に規定されており、要約すれば図表3のようになる。

図表3　秘密保護法による罰則

条文	対　象　・　違　反　形　態	罰　　則
3条	1項1号　わが国の安全を害する用途に供する目的をもって、又は不当な方法で、特別防衛秘密を探知し、又は収集した者	10年以下の懲役
	1項2号　わが国の安全を害する目的をもって、特別防衛秘密を他人に漏らした者	
	1項3号　特別防衛秘密取扱者で、その業務により知得し、又は領有した特別防衛秘密を他人に漏らした者	
	2項 1項2号又は3号に該当する者を除き、特別防衛秘密を他人に漏らした者	5年以下の懲役
4条	1項 特別防衛秘密取扱者で、その業務により知得し、又は領有した特別防衛秘密を過失により他人に漏らした者	2年以下の禁錮又は5万円以下の罰金
	2項 特別防衛秘密取扱者以外で、その業務により知得し、又は領有した特別防衛秘密を過失により他人に漏らした者	1年以下の禁錮又は3万円以下の罰金
5条	1項 上記3条1項を陰謀、教唆又は扇動した者	5年以下の懲役
	2項 上記3条2項を陰謀、教唆又は扇動した者	3年以下の懲役
6条	自首したときは、その刑を軽減又は免除する	

（出所）筆者作成

つまり、防衛庁・自衛隊関係者が扱う情報に関していえば、防衛庁が秘密として管理しているもの（「庁秘」と呼び、その中がさらに機密・極秘・秘に分かれる）に加え、防衛秘密と特別防衛秘密があることになる。これらの目的や刑罰を比較すると、図表 4 のようになる。

図表 4　防衛庁・自衛隊における秘密の分類

区分 / 事項	庁　　秘	防 衛 秘 密	特別防衛秘密
目　　的	服務規律維持	秘密保護	秘密保護
主 対 象 者（正犯）	職務上秘密を知り得た隊員	防衛秘密を取り扱うことを業務とする（した）以下の者 ① 防衛庁職員 ② 国の行政機関の職員 ③契約業者	特別防衛秘密を取り扱うことを業務とする（した）以下の者他 同左
罰 則 規 定	1 年以下の懲役他	5 年以下の懲役　他	10 年以下の懲役　他
未遂・過失の取扱い	処罰せず	未遂・過失も処罰	未遂・過失も処罰
国外犯の規定	なし	日本国民の国外犯について規定	なし

（出所）筆者作成

３．通信の秘密

ここで若干回り道をするようだが、主体による分類を一旦離れて、過程による分類のうちデジタル情報の利用度が高い、通信ネットワークにおける秘密保護を見ておこう。われわれが平和な毎日を送るための大前提は、通信の違法な傍受や検閲が行なわれることなく、通信に関する「秘密の保持」が担保されていることであろう。電気通信事業法[17] 3 条、4 条、179 条は、それぞれについて、次のように規定する[18]。

（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。
（秘密の保持）
第 4 条　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。
第179条　電気通信事業者の取扱中に係る通信（第 164 条第 2 項に規定する通信を含む）

[17] 「電気通信事業法」（1984 年法律第 86 号）。
[18] なお、通信の秘密保持の規定は有線電気通信法や無線法にも存在するが、図表 5 のようにその間の整合は取れていない。

の秘密を侵したものは、2 年以下の懲役又は 100 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には、3 年以下の懲役又は 200 万円以下の罰金に処する。
3 前 2 項の未遂罪は、罰する。

憲法第 21 条第 2 項は、「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。」と規定し、基本的人権のうち最も重要なものの一つである言論の自由を、不当に圧迫する惧れのある検閲などを禁止している。上記の諸規定は、この憲法の規定を受けて設けられたものである[19]。

憲法の規定は直接的には国の機関、その他の公の機関が、通信の内容を調べることを禁止したもので、「検閲」とは、公権力が外部に発表されるべき思想内容を、あらかじめ審査し、不適当と認めるときはその発表を禁止する行為である。私企業であるコモン・キャリアは、これによって直接規律を受ける訳ではない（NTT 東西両会社のような特殊会社については議論があるかも知れない)。事業者については、個別法である電気通信事業法における検閲禁止（同法 3 条）や秘密保護（4 条）の趣旨と同時に、利用の公平（6 条）を踏まえた契約約款（19 条以下）あるいは個別契約によって律せられることになる。

また電気通信事業者でなくても、有線・無線の通信を行なう者は、その通信の秘密を守らなければならず、違反行為に対しては刑事罰の対象となる（有線法[20] 9 条、電波法[21] 59 条)。ここで無線通信は有線通信と違って傍受の意図がなくても偶然傍受してしまうことがあり得るから、両者の構成要件が違うのは当然とも言える。しかし図表 5 に掲げるような差（とりわけ刑の軽重）がそのまま是認されるか否かは、疑いの余地なしとしない。前述の防衛秘密を犯す罪、電気通信事業者の秘密侵害罪、国家公務員の守秘義務違反などを横断比較した考察が望まれる。

図表 5　通信の秘密に関する実体法と罰則規定

法	業　法	基　本　法	
実 体 法	電気通信事業法 3 条、4 条	有線法 9 条	電波法 59 条
	（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。	（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 164 条第 2 項 の通	（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

19 通信の秘密保持を理論づけるには複数のアプローチがあるが、「言論の自由の保障を実効性あらしめるため」という説明も十分根拠のある立論だと思われる。ところが不思議なことに、「言論の自由」を世界一重視しているはずのアメリカ合衆国憲法には、歴史的な事情もあってか「通信の秘密保持」の規定はなく、通信傍受はかなり幅広く行なわれている（傍受そのものは犯罪とならず、「傍受し漏洩」すれば犯罪となる、連邦通信法 705 条)。

20 「有線電気通信法」(1953 年法律第 96 号)。

21 「電波法」(1950 年法律第 131 号)。

	（秘密の保護） 第 4 条　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。	信たるものを除く。）の秘密は、侵してはならない。	4 条第 1 項 又は第 164 条第 2 項の通信であるものを除く。第 109 条並びに第 109 条の 2 第 2 項及び第 3 項において同じ。）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。
罰則規定	179 条、164 条 2 項	14 条、15 条	109 条、109 条の 2
	第 179 条　電気通信事業者の取扱中に係る通信（第 164 条第 2 項に規定する通信を含む。）の秘密を侵した者は、2 年以下の懲役又は 100 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、3 年以下の懲役又は 200 万円以下の罰金に処する。 3 前 2 項の未遂罪は、罰する。 （適用除外等） 第 164 条 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 14 条　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、2 年以下の懲役又は 50 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、3 年以下の懲役又は 100 万円以下の罰金に処する。 3　前 2 項の未遂罪は、罰する。	第 109 条　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 50 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 100 万円以下の罰金に処する。 第 109 条の 2 暗号通信を傍受した者又は暗号通信を媒介する者であって当該暗号通信を受信したものが、当該暗号通信の秘密を漏らし、又は窃用する目的で、その内容を復元したときは、一年以下の懲役又は五十万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、前項の罪を犯したとき（その業務に関し暗号通信を傍受し、又は受信した場合に限

			る。）は、二年以下の懲役又は百万円以下の罰金に処する。 3 前 2 項において「暗号通信」とは、通信の当事者（当該通信を媒介する者であって、その内容を復元する権限を有するものを含む。）以外の者がその内容を復元できないようにするための措置が行われた無線通信をいう。 4 第 1 項及び第 2 項の未遂罪は、罰する。

（出所）筆者作成

一般に「通信の秘密」として保護される対象には、通信の内容はもちろん、通信の当事者（発信人、受信人）の居所、氏名、発信地・受信地、通信回数、通信年月日などが全て含まれる。これらは通信の意味内容をなすものではないが、通信そのものの構成要素であり、これらの事項を知られることによって、通信の意味内容が推知されるからである。

なお、従来暗号化された通信を他と区別する法制はなかったが、サイバー犯罪条約[22]との整合性を意識した 2004 年の電波法改正において「暗号通信復元罪」（電波法 109 条の 2）が新設されたことが注目される。これは電波法の規定であるから、無線通信についてしか適用がない。有線通信の場合は、傍受行為が通信の秘密を侵害するものとして処罰の対象になる（無線の場合は傍受するだけでは処罰されない）から、このアンバランスは是認されるということだろうか。この点も、より突っ込んだ検討が必要と思われる[23]。

ところで、通信が犯罪などに関連しているときは、通信の秘密の保障と捜査上の要請との調和について、難しい問題が生ずる。脅迫犯人が現に発信している電話を、被害者の要請によって電気通信事業に従事する職員が逆探知し、捜査機関に通報するような場合は、本項の規定に違反しないものと解されている[24]。しかし実際には、電電公社およびNTTは、「通信の秘密」を厳格に把えていたこともあり、被害者の要請だけで逆探知を行なったケース

[22] 欧州評議会で策定された条約だが、わが国も署名。これを受けた「犯罪の国際化及び組織化並びに情報処理の高度化に対応するための刑法等の一部を改正する法律案」は現在国会審議中。

[23] 加えて、不正アクセス行為無くして暗号の解読は不可能だろうし、有線通信の部分が全く無く、オール無線のネットワークは極めて稀であることから、後述の不正アクセス禁止法で有線通信の暗号解読には十分対応できるとの見方もあり得よう。しかし、そもそも有線と無線を峻別することが意味を成さないほどになっているのだから、共通法をまず考え、その後両者に固有の規定が必要なら追加する、との発想の転換が望まれる（林[2005b]）。

[24] 電電公社時代に内閣法制局意見として、「脅迫の罪を現に犯している者がある場合において、被害者の要請があるときは、公社の職員が当該電話の発信場所を探索し、これを捜査官憲に通報することは許される」（つまり令状がなくても良い）とする見解が示されていた（1963 年 12 月 9 日法制局 1 発 24 号）。

は年に 1〜2 件程度で、原則としては裁判所の令状を待って行なわれていたという（令状主義・林[2005b]）。

このように、わが国の場合通信傍受は極めて限定的であったが、いわゆるハイテク犯罪や国際マフィアによる犯罪などが顕在化してくると、従来のような固定的な発想だけでは社会秩序が守られなくなった。そこで、捜査機関による通信や会話の秘密裡の傍受が、憲法上果たして許されるか、許されるとすればいかなる条件の下に許されるのかを検討した上で、「通信傍受法[25]」が制定され 2000 年 8 月から施行された。

この法律は、組織的な犯罪が増加し、通信の傍受なくしては十分な対応ができない状況に対処しようとするものであり、対象とする通信は電話、ファクシミリ、コンピュータ通信などの電気通信（伝送路の全部又は一部が有線であるもの又は伝送路に交換設備があるもの）である。しかし対象犯罪は、必要最小限のものとするため、通信傍受という新たな捜査方法が必要不可欠と考えられる、組織的な犯罪（組織的な殺人、薬物・銃器関連犯罪、集団密航に関する罪）に限定されている（同法 1 条、具体的罪名は別表にあるが省略）。

ここで令状（傍受令状）発出の要件は、同法 3 条に詳細に規定されており[26]、このような規定は「裁判官の事前の令状による」という大原則を崩したものではない。しかし 12 条で定められた通信事業者等の立会いや意見陳述は、これまでのC型規律（コモン・キャリアは通信内容にタッチしないという規律）をアメリカ的なC´型規律に変質させる要素を含んで

---

[25] 「犯罪捜査のための通信傍受に関する法律」（1999 年法律第 137 号）。

[26] 令状発出の要件は

① 下記アからエについて犯罪の高度の嫌疑があり、当該犯罪が数人の共謀によるものと疑うに足りる状況があること（同 3 条 1 項各号）
　ア 対象犯罪が犯された場合
　イ 対象犯罪が犯された後も同一又は同種の対象犯罪が犯される場合
　ウ 当該犯罪の実行を含む一連の犯行の計画に基づき、対象犯罪が犯される場合
　エ 死刑又は無期若しくは長期 2 年以上の懲役・禁錮に当たる罪が、対象犯罪と一体のものとしてその実行に必要な準備のために犯され、引き続き対象犯罪が犯される場合
② 犯罪の実行に関連する事項を内容とする通信（犯罪関連通信）が、行なわれると疑うに足りる状況（同 3 条 1 項本文）
③ 他の方法によっては、犯人の特定、犯行の状況・内容を明らかにすることが著しく困難（同上）
④ 傍受対象の通信手段は、犯人による犯罪関連通信に用いられると疑うに足りるもの（同上）

となっている。

請求権者は、検事総長が指定する検事、または国家公安委員会等が指定する警視以上の司法警察員等、発布権者は地方裁判所裁判官に限定されている（同 4 条）。また傍受の期間は 10 日以内で（同 5 条）、地裁裁判官が必要があると認めるときは、請求によって 10 日以内の期間を定めて延長可能であるが、通算して 30 日を越えることはできない（同 7 条）。再請求は、さらに傍受を必要とする特別の事情を要する（同 8 条）。

なお、傍受の実施における適正確保のため

① 通信手段の傍受を実施する部分を管理する者に令状を提示し（同 9 条）、
② 通信手段の傍受を実施する部分を管理する者または地方公共団体の職員（例：消防署の職員）の常時立会いが必要であり（同 12 条 1 項）、
③ 立会人は傍受実施に関し意見を述べることが可能（同 2 条）

となっている。

また、傍受の対象は傍受令状で指定された通信のほか、傍受すべき通信に該当するか否かの判断に必要な最小限度に限ることとしている（同 13 条）。

いることは間違いない(林[2005b])[27]。

ところでこの法律に関しては、その法案提出と平行して、「盗聴法」という名のレッテルを貼ったイデオロギー運動が展開された[28]。その論点を要約すると、おおよそ次のような諸点になるであろう（奥平[2001]、岩村[2001] 参照)。

①（憲法の実体規定として）「検閲の禁止」「通信の秘密保持」（憲法 21 条 2 項）は、絶対的禁止規定か。絶対的でないとすれば、

②（憲法の手続き規定として）裁判所の検証令状を得て行なわれれば、「令状主義」「適正手続き」（憲法 31 条、35 条）に適っており合憲と考えてよいか。その際、

③（伝統的な法体系に照らし）令状は有体物に限ると考えるべきか。そうだとすれば、ファックス送信紙などは有体物であるが、音声は入らないので、

④無体物の押収等はおよそ不可能なのか、憲法 31 条の適正手続きに戻って判断すべきか。

⑤（仮に無形物の押収も令状により可能との立場を採った場合）令状を事前に相手方に示さねばならないか。

⑥（同じ条件の下で）捜査対象である物や場所の特定は、どの程度要請されるか。

⑦通信傍受は既に行なわれた犯罪の証拠を収集するのではなく、将来起こり得る犯罪に対応するためのものであり、そもそも容認し得るものなのか。

⑧この点を拡大していくと、別件による傍受が際限なく行なわれる危険があるが、どこまでなら許容されるか。

ここで奥平説は（あるいは右崎・川崎・田島（編）[2001]の執筆陣はほぼ揃って）①において「絶対的禁止説」を採るようである。この説を採れば、上記で多数挙げた判断ボックスの最初のところで通信傍受を全面的に否定しているので、その後の議論は全く意味を成さないことになる。

また論者は、仮に①～④までを認めるにしても、⑤は譲れない要件だと主張するが、それは「被疑者に事前通知の上で通信を傍受する」というナンセンスな状態を示すものに他ならない。加えて、固定電話は対象だが携帯電話は対象外なので、不平等扱いだと主張するが、それなら携帯電話を含める主張をされてはいかがかと思う。

この論文は 9 月 11 日事件以前に書かれたものであるため、論者の見方はその後変化したのかも知れない。しかし、依然としてこの説に固執されているのであれば、「平和ボケ」と言うしかあるまい。通信傍受法の実体は、基本的人権を守るという面では安心であるが、「盗

---

[27] メディア関連産業は、経済的規制（参入・退出規制や料金規制）の有無と、社会的規制（コンテンツ規制）の有無によって 4 パターンに区分できる。両者とも「あり」が放送業（B型）で、両者とも「なし」が新聞・出版業（P型)、前者が「あり」後者が「なし」が電気通信業（C型）であった。ところがプロバイダ責任（制限）法などの施行に伴って、従来コンテンツに責任を負わなかったC型が、一部責任を負うC´型へと変化しつつある。

[28] 奥平[2001]は、法案提出者が「盗聴と呼ばず傍受と呼んで欲しい」と要請したことに対して、これをイデオロギー的言明だと断罪するが、同じ文脈で「傍受と呼ばず盗聴と呼ぶ」こともまた、イデオロギー的言明に他ならないであろう。とりわけ小田中[2001]が、地方分権一括法などを含めて、「戦後民主主義の構造的解体を指向する」「クーデター的」悪法と評するのは、イデオロギーそのものである。問題は、「個々のケースにおける傍受が合法か違法か」にあるのであって、「傍受一般が合法か違法か」にあるのではない。

聴法」という名称を与えようにも、実際は盗聴どころか犯罪捜査のための本来の傍受さえ不可能なのが現状と思われる[29]。

だが、その対策となると意見が分かれる。法改正によって、より実効性のある方法を模索するのか、そもそもインターネットについては傍受は実効性がないとあきらめるのか（牧野[2001]）。われわれは、真剣な検討を求められていると言えよう。

同様の問題を提起しているのが、「プロバイダ責任（制限）法[30]」における発信者情報開示の是非である。たとえばインターネットの掲示板などに、名誉毀損とおぼしき書き込みがある場合、書き込んだ当人は通常匿名や変名である。わが国の訴訟手続では、訴えの提起には被告人を特定し、訴状を送達できるようにしなければならないので（民事訴訟法 133 条、138 条）、これでは訴訟を起こすことができない。そこで被害を主張したい側は、発信者が誰であるかを（少なくとも加入手続等を通じて）知っているはずのプロバイダ(ISP=Internet Service Provider)に、発信者情報の開示を求めることになる（プロバイダ自体の管理者責任を問う訴訟も可能であるが、ここでは深入りしない）。

前述の如く、発信者の情報も通信の秘密の一部を構成するから、これを無制限に公表したのでは通信の秘密が無意味になる。さりとて被害者が裁判を受ける権利も無視することはできない。この両者のバランス調整に配慮した「プロバイダ責任（制限）法」は、次のように規定する。

（発信者情報の開示請求等）

第 4 条 特定電気通信による情報の流通によって自己の権利を侵害されたとする者は、次の各号のいずれにも該当するときに限り、当該特定電気通信の用に供される特定電気通信設備を用いる特定電気通信役務提供者（以下「開示関係役務提供者」という。）に対し、当該開示関係役務提供者が保有する当該権利の侵害に係る発信者情報（氏名、住所その他の侵害情報の発信者の特定に資する情報であって総務省令で定めるものをいう。以下同じ。）の開示を請求することができる。

一　侵害情報の流通によって当該開示の請求をする者の権利が侵害されたことが明らかであるとき。

二　当該発信者情報が当該開示の請求をする者の損害賠償請求権の行使のために必要である場合その他発信者情報の開示を受けるべき正当な理由があるとき。

2　開示関係役務提供者は、前項の規定による開示の請求を受けたときは、当該開示の請求に係る侵害情報の発信者と連絡することができない場合その他特別の事情がある場合を除

---

[29] 通信傍受の実施状況について、政府は毎年請求・受付件数や罪名、実施機関、通信回数などを国会に報告しなければならない（同法 29 条）。それによれば、2003 年度中の請求・受付件数は 2 回にまとめて 4 件で、いずれも麻薬・覚せい剤関係の犯罪に関するものであった。

[30] 「特定電気通信役務提供者の損害賠償責任の制限及び発信者の情報開示に関する法律」（2001 年法律第 137 号）。なお本法の略称として、立法者は「プロバイダ責任制限法」という呼称を推奨している。確かに立法趣旨が責任の制限にあることは確かだが、実務上は制限していることになるのか、逆に責任を新たに負荷しているのか分からないので、私は本文の表記に統一している。

き、開示するかどうかについて当該発信者の意見を聴かなければならない。
3　第一項の規定により発信者情報の開示を受けた者は、当該発信者情報をみだりに用いて、不当に当該発信者の名誉又は生活の平穏を害する行為をしてはならない。
4　開示関係役務提供者は、第一項の規定による開示の請求に応じないことにより当該開示の請求をした者に生じた損害については、故意又は重大な過失がある場合でなければ、賠償の責めに任じない。ただし、当該開示関係役務提供者が当該開示の請求に係る侵害情報の発信者である場合は、この限りでない。

条文としては良く練られていると思われるが、実際の解釈においては裁判官のインターネットに関する知識が十分でないためか、やや安易に発信者情報の開示がなされている、との懸念がある（林[2005b]）。たとえば、医療法人メディアカル・ドラフト会議事件[31]では、紛争当事者がお互いを認識し対話まで行なわれているのに、加害（推定）者の発信IDが会社のものと同じであれば「会社ぐるみ」の犯罪であることが立証できるとする（実際は、その両者は必ずしも同一ではないが）被害（推定）者の主張を容れて、開示が命じられた。またパワードコム事件[32]では、ピア・ツー・ピアの通信によるファイル交換は、複数のISPを経由しているところ、仲介するだけのISPにも発信者情報開示が命じられている。
今後判例の積み重ねを通じて、通信の秘密と公平な裁判を受ける権利のバランスを追求していく必要があろう。

４．企業の秘密

さて回り道から本来の議論に戻ろう。秘密を主体別に考えた場合の第 2 の類型は、企業の有する秘密であり、現行法では「営業秘密」が直接これに該当する。ただし後述するように、「公開（あるいは登録）して権利を守る」という場合の客体も、広義の秘密に該当するのだという立場に立てば、知的財産一般がこの範疇に属することになる。
不正競争防止法[33] 2 条 4 項によれば、営業秘密とは「秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないもの」であり[34]、同条 1 項 4 号から 9 号では、以下の行為が「不正競争」として禁じられている。

（定義）
第 2 条 四　窃取、詐欺、強迫その他の不正の手段により営業秘密を取得する行為（以下「不

[31] 東京地判 2003 年 3 月 31 日、最高裁判例情報・下級審主要判決情報 http://courtdomino.courts.go.jp/kshanrei.nsf
[32] 東京地判 2003 年 9 月 12 日、平成 14 年(ワ)28169 号。最高裁判例情報・下級審主要判決情報 http://courtdomino.courts.go.jp/kshanrei.nsf
[33] 現行法は注 1 にある如く 1993 年制定、1994 年施行。同名の旧法は 1934 年法律第 14 号。
[34] 本稿の冒頭に掲げた「有用」「非公知」「秘密管理」の 3 要素がすべて含まれていることに、改めて注意を喚起しておこう。

正取得行為」という。）又は不正取得行為により取得した営業秘密を使用し、若しくは開示する行為（秘密を保持しつつ特定の者に示すことを含む。以下同じ。）

五　その営業秘密について不正取得行為が介在したことを知って、若しくは重大な過失により知らないで営業秘密を取得し、又はその取得した営業秘密を使用し、若しくは開示する行為

六　その取得した後にその営業秘密について不正取得行為が介在したことを知って、又は重大な過失により知らないでその取得した営業秘密を使用し、又は開示する行為

七　営業秘密を保有する事業者（以下「保有者」という。）からその営業秘密を示された場合において、不正の競業その他の不正の利益を得る目的で、又はその保有者に損害を加える目的で、その営業秘密を使用し、又は開示する行為

八　その営業秘密について不正開示行為（前号に規定する場合において同号に規定する目的でその営業秘密を開示する行為又は秘密を守る法律上の義務に違反してその営業秘密を開示する行為をいう。以下同じ）であること若しくはその営業秘密について不正開示行為が介在したことを知って、若しくは重大な過失により知らないで営業秘密を取得し、又はその取得した営業秘密を使用し、若しくは開示する行為

九　その取得した後にその営業秘密について不正開示行為があったこと若しくはその営業秘密について不正開示行為が介在したことを知って、又は重大な過失により知らないでその取得した営業秘密を使用し、若しくは開示する行為

ここで営業秘密に当るか否かは、本稿冒頭で「秘密」の要件として掲げた(1)有用性、(2)非公知性、(3)秘密管理性の観点から検討しなければならない。

(1)有用性

有用性の趣旨について、立法担当者は、「法的保護を行なうに足る社会的意義と必要性があるものに保護の対象を限定することとし、このため、事業活動に有用な技術上又は営業上の情報であることを要件としたものである。したがって、スキャンダル情報等のように事業活動に有用なものとはいい難い情報は保護の対象外となる」と述べている（通産省知的財産政策室[1990]）。

(2)非公知性

既に知られている情報はもとより、一般に知られ得る情報は、営業秘密として保護されない。この点に関しては立法当時から、ある技術情報が利用された製品を解析することによって、当該情報を探知することができる（リバースエンジニアリング）場合に、非公知性を失うかどうかという問題が議論されてきた。

一般に、情報を不正な手段によらずに取得することは可能であるが、それに相当な時間

や費用がかかるときには、当該情報は非公知性の要件を満たすと解されよう。そのような情報は、保有者に時間や費用の点から比較優位を与えるもので、保護されるべき価値があり、また不正行為に対する保護を認めても情報の円滑な流通・利用を阻害することにはならないからである（茶園[2004]）。

営業上の情報である顧客情報に関しては、誰が顧客であるかを、一般にアクセスしうる名簿等から容易に推測することができる場合には、その顧客情報は公知であり、営業秘密として保護されない。これに対して、誰が顧客であるか自体が一般に知られていない場合には（たとえば男性用かつらの顧客[35]）、その顧客情報が非公知性の要件を満たすことになる。

(3)秘密管理性

営業秘密の 3 番目の要件は、「営業秘密が秘密として適切に管理されていなければならない」（秘密管理性）ということである。この要件が必要なのは、保護を受けるべき情報とそうでない情報が明確に区別されていなければ、情報の取得や使用・開示を行なおうとする者にとって、当該行為が不正行為となり差止の対象となり得るか否かについての、予測可能性が損なわれるからである（通産省知的財産政策室[1990]）。

多くの裁判例では、この要件を満たすためには、当該情報にアクセスできる者が制限されていること（「アクセス制限」）と、当該情報にアクセスした者に当該情報が営業秘密であることを認識できるようにしていること（「客観的認識可能性」）の両方が必要であるとされている。そして、必要とされる秘密管理の程度や態様は、この要件の趣旨からして、画一的な基準があるのではなく、「情報の性質、保有形態、企業の規模等」に応じて決定され、また情報を利用しようとする者が誰であるか、とりわけ情報を保有する企業の従業員であるか外部者であるかによって、異なると解されている。

かくして、3 つの要件が満たされる場合には、当該情報は「営業秘密」としての保護対象になり、その不正利用行為は禁止される。ここでは、後述する個人情報と関係の深い顧客情報の不正利用行為について、営業秘密としての保護のあり方を見ていこう。

営業秘密である顧客情報を使用したか否かは、当該情報を保有する者しか知らない顧客への売り込みがあったり、偶然とはいえない程に顧客が重なっていること等の事情から、推定できる場合がある。他方、取引を勧誘した顧客が公知資料から容易に推測できる場合には、営業秘密の使用が否定される場合が多いだろう。

元従業員が在職中に自ら入手した顧客情報を使用する行為が、不正競争になるかどうかが争われた裁判例はいくつかある。ここで、従業員が自ら創作したり入手した情報を使用する行為が、営業秘密の保有者「からその営業秘密を示された」ことを要件とする 2 条 1 項 7 号の対象となるか否かについて、学説上の争いがある。一方の説は、そのような情報

[35] 大阪地判 1996 年 4 月 16 日知財集 28 巻 2 号 300 頁。いわゆる「男性用かつら顧客名簿事件」として知られる有名な事件。

は従業員が使用者から示されたものではないために同号に該当しないとし、他方の説は、営業秘密の「帰属」を問題として、営業秘密が使用者に帰属する場合には 7 号に該当する場合があるとする。

しかし実態的には、いずれの見解をとっても結論はあまり変わらないであろう[36]。前説によれば、このような顧客情報について使用者が保護を受けるためには、契約で従業員に対して秘密保持義務を課すことになる。他方後説でも、当該情報が不正競争防止法によって保護されるには、秘密管理性の要件が満たされる必要があり、そのためには、従業員に明確な秘密保持義務が課されていなければならないからである（茶園[2004]）。

営業秘密の不正利用行為に対しては、それにより営業上の利益を侵害され又は侵害される惧れのある者はその差止を請求することができる（3 条 1 項）。技術的な情報の不正使用に対しては、当該情報を使用した製品の製造販売の差止請求、顧客情報の不正使用に対しては、当該情報に含まれる者への取引勧誘などの差止請求が一般的である[37]。

故意又は過失による営業秘密の不正利用行為により営業上の利益を侵害された者は、これによって生じた損害の賠償を請求することができる（4 条）。不正競争防止法 5 条は、損害額の推定等について規定しているが、2003 年改正により新設された同条 1 項が適用された例は未だないようである。

一方、営業秘密の侵害に関する刑事法上の保護はどうなっているのだろうか。2003 年の不正競争防止法改正で、営業秘密侵害罪の規定が初めて盛り込まれたが（同法 14 条 1 項 3 号～6 号）[38]、それ以前にも、企業秘密の漏洩事件をめぐる幾つかの刑事判例があった。

過去の判例では、①会社の秘密資料を持ち出すなどの不法な手段・方法を、窃盗罪や詐欺罪などで捕捉した事例（大日本印刷事件[39]など）と、②内部者による横領の類型とした事例（鐘淵化学事件[40]、など）のほか、③背任罪の成立を肯定した珍しい例として、綜合コン

---

[36] 田村[1996][1999]は、「帰属」に関する議論そのものに意味が無いとするが、ここでは深入りしない。

[37] これに対して、前述の男性用かつらの顧客名簿の不正利用に関する判決では、「別紙顧客目録記載の者に対し、面会を求め、電話をし又は郵便物を送付するなどして、男性用かつらの請負若しくは売買契約の締結、締結方の勧誘又は理髪等同契約に付随する営業行為」を行なうことの差止請求のみならず、「男性用かつらの請負若しくは売買契約の締結をしようとし又は理髪等同契約に付随するサービスの提供を求めて被告宛来店あるいは電話連絡をしてくる別紙顧客目録記載の者に対し、男性用かつらの請負若しく売買契約の締結、締結方の勧誘又は理髪等同契約に付随する営業行為」を行なうことの差止請求も認容された。

これは不正競争防止法上の保護を超えるものとも言えるが、この事案では男性用かつらの顧客獲得には効果的な宣伝広告が不可欠であるが、被告はほとんど宣伝広告を行なっていないために、顧客が自発的に被告との取引を求めて来店や電話連絡してきても、それは被告が先に行った原告の顧客名簿に基づく勧誘の結果に他ならないという特殊な事情があったのであり、営業秘密の実効的な保護を図るものとして支持する意見が多い（田村[1996][1999]）。

[38] 1974 年の改正刑法草案において「企業秘密漏示罪」の新設が提案されたが（同草案 318 条）、改正刑法草案全体が「処罰権の拡大」や「重罰化」という批判を受けたこともあり、「企業秘密」の保護立法も見送られる結果となった。その後も、産業界による法的保護の要請が繰り返される一方、近年の急速なコンピュータ化に伴い、新たに財産的情報の取り扱いが問題になった。それらは、1999 年の不正アクセス行為禁止法などによる電子データの保護に結びついている。もちろん、企業秘密または営業秘密の侵害行為を刑罰で禁止することに対しては、依然として消極論が根強いものの、国際的な保護法制の平準化もあって、諸外国の法制度に近づける形で、刑法的保護を実現する素地が用意された（佐久間[2004]）。

[39] 東京地判 1965 年 6 月 26 日。下級刑集 7 巻 6 号 1319 頁。判時 419 号 14 頁。1966 年 9 月 17 日控訴棄却。

[40] 大阪地判 1967 年 5 月 31 日。判時 494 号 74 頁。判タ 209 号 260 頁。

ピュータ事件[41]が挙げられる、という（佐久間[2004]）。

①と②の類型は、有体物を念頭においた現行刑法典の下では、侵害行為の外形を捉えて、窃盗罪や横領罪で処罰する他はないための便法であると考えられる。他方背任罪については、同罪の成立要件が相当に厳格であるため、各種のデータやノウハウなどの窃取については、「刑事法上の罰則がない」と評される状態が続いてきた。

1990 年の不正競争防止法改正では、営業秘密の保護を求める国際潮流に合わせて差止請求権や損害賠償請求権を含む民事上の手当がなされたが、この時点でも、刑事罰の新設は見送られた。刑事罰は 2003 年の不正競争防止法改正において、やっと実現することになったが、ここでも刑法の伝統に従い営業秘密という不定形な対象を定義するのでなく、不法領得ないし不正使用・開示などの侵害形態に着目して、処罰の範囲と限界を明らかにしようとしている。

その態様は、前述の 3 つの類型に対応している。まず不正競争防止法 14 条 1 項 3 号は、営業秘密不正取得後使用・開示罪として、詐欺・恐喝・強盗などの「詐欺等行為」と、窃盗・住居侵入・不正アクセスなどの「管理侵害行為」を手段とする場合を規定している。次に同項 4 号では、3 号の準備的行為の中でも、法益侵害に直結する違法性の高いものだけに限定して（窃盗・詐欺・横領・不正コピー）、営業秘密記録媒体等不正取得・複製罪とした。

さらに同項 5 号では、横領にあたる形態として営業秘密記憶媒体等不法領得後使用・開示罪を設けている。すなわち、同号のイ類型は、一部で有体物の窃盗・詐欺にあたる「領得」の形態を取り込むが、同号のロ類型は、たとえ部外者（退職者を含む）にあたる場合にも、かつて正当に「営業秘密を保有者から示された者」が、その後不正コピーを通じて営業秘密を侵害する例が少なくない点に着目し、いわば正当取得類型と不正取得類型の交差領域にあたるものと説明されている（経産省知的財産政策室[2003]）。

これに対して、同法 14 条 1 項 6 号が規定する営業秘密正当取得後不正使用・開示罪は、完全な背任類型であって、現役の役員または従業員が、彼らの負担する守秘義務に違反して使用・開示した場合を処罰の対象とする。しかし、ここで注目すべき点は「役員」と「これらに準ずる者」に加えて、行為主体に「従業者[42]」を列挙したことである。

この営業秘密はあくまで秘匿が前提であるので、情報公開が前提になっている知的財産制度とは、全く逆方向にあるように見える。しかし既に触れたように、企業は秘匿か公開かの選択肢を持っているし、不正競争防止法自体を知的財産制度全般の中で考察する論者も多い（田村[2003]は営業秘密を特許権における発明や著作権における著作物と同列に扱っているが、紋谷[2003]は権利侵害の一態様として扱っている）。ここで知的財産制度の中でも、特許権と著作権の間には図表 6 のような対照的な差異があることに留意しなければならない。この図表には、かつてプログラム権法として検討された内容が参照モデルとし

[41] 東京地判 1985 年 3 月 6 日。判時 1147 号 162 頁。判タ 553 号 262 頁。
[42] これは法律の文言であるので、本文の一般例である「従業員」という用語は使わない。

て挿入されている。

図表 6 特許権・著作権・プログラム権の比較

権利の種類と根拠法	権利の発生	保護期間	保護対象	強制許諾	取得費用	域外適用
特許権 (特許法)	出願・設定の登録	出願日から20年	アイディア	有	(米) 1万ドル (日) 50～60万円	なし
著作権 (著作権法)	著作行為 (無方式)	著作者の存命中及び死後50年	表現	無	ゼロ	? (ベルン条約加盟国間)
(参考) プログラム権 (1985年当時の「プログラム権法」の考えによる)	登録	15年程度	プログラム製品(人格権は認めず、使用権という概念を導入)	法制定により可	僅少	?

(出所)筆者作成

これらの詳細は別の文献をご参照いただくしかないが(前者については中山[1993]、後者については林(編著)[2004]、林[2005a]など)、ここでの論点は公開の程度(費用を含む)と権利保護期間の長短の関係である。特許権は、特許を取得したい発明の範囲を明確にして特許庁に出願し(特許法 36 条)、その審査を経て(47 条)、設定の登録をすることによって権利が発生し(66 条)、その期間は出願後 20 年であり(67 条)、毎年所定の登録料を支払わねばならず(195 条 2 項ほか)、しかも出願の内容は審査請求(48 条の 2)の有無にかかわらず、出願から 18 ヵ月を経過すると公開されてしまう(64 条)[43]。

これに対して著作権は、なんらの要式行為を伴わず権利が発生し(無方式主義、著作権法 17 条 2 項、51 条 1 項)、その期間も一般的には著作者の存命中プラス死後 50 年と、特許権に比べて圧倒的に長い(51 条 2 項ほか)。無方式であるから、もちろん登録料も発生せず、著作者あるいは著作権者にとっては有利である。80 年代半ばに、ソフトウェアを特許権で保護するか著作権によるかが国際的な激しい論議を呼んだ際、アメリカが著作権を強く支持したのは、この権利保護の強さであったというのは肯ける[44]。

このような中で、営業秘密については、旧不正競争防止法(1934 年法律第 14 号)施行当時はもとより、1990 年の改正により営業秘密が保護対象になった際も、民事的な救済(差止、損害賠償)が認められるに過ぎなかったが、新法の施行(1994 年)から 10 年を経た 2004

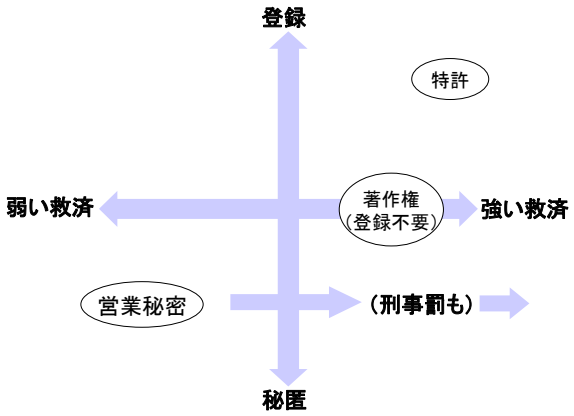
[43] 戦後の日本においては、秘密特許制度(特許は与えるが秘密にする)は廃止され、日米防衛特許協定に基づくものだけが残っている(山名[2004])。しかし諸外国においては、軍事上必要な発明に関する特許について特別な扱いをすることは広く認められている。

[44] アメリカはその後、著作権の保護期間を 20 年延長し、現在では一般的な著作物は著者の存命中と死後 70 年、法人著作物は公表後 95 年保護されることになっている。

年の改正において刑事罰も科されることになった（14 条 1 項 3 号～6 号）ことは既に述べたとおりである。本稿の文脈では、営業秘密の重要性がより広く認知された結果と評価できなくもない。しかし、上記の特許と対比してみると、登録などによる公開とは対局にある情報（＝秘密）が、それほど強く守られてしかるべきか否かは、議論の余地を残している。

ここで図表 7 を描いてみると、この間の事情を視覚的に理解することができよう。つまり公開（登録）に近い情報は、権利者以外も情報に接し、許諾を得れば利用の道が開かれているのだから、その侵害に対して刑事罰を含む強い救済を与えてもよかろう。しかし、秘匿に近い情報が侵害された場合は、契約書に基づく弱い救済の道（たとえば NDA=Non Disclosure Agreement を結んだ情報を漏洩した場合には、債務不履行に問われるという）があるのは当然としても、刑事罰も含めた強い救済が認められるのが妥当か否かは、多分にイデオロギーの領域に属すると考えられるからである。

図表 7　情報と保護方法の分類



（出所）筆者作成

（注）ソフトウェアは、著作権で保護されると同時に、論理構造に新規性と進歩性があれば、特許権でも保護される。

なおここで「強い」「弱い」という相対的表現をしたのは民事と刑事でどちらが強い救済かは、被害者の主観によること。加えてプログラムや著作物の場合には、コピーガードなどの技術的保護手段を回避すること自体が禁じられ(不正競争防止法 2 条 1 項 10 号･11 号。著作権法 120 条の 2)、これが最も強いと考えられるからである。前述の無線通信における「暗号通信復元罪」にも対比できよう。

この問題は、著作権について「より権利を強めることが創作のインセンティブを通して社会全体の効用を高める」とする派（プロ・コピーライト）と「より自由な利用こそが、第 2 の著作や 2 次的な著作物を通じて社会全体の効用を高める」とする派（コピーレフトやフリーソフト運動)に分断されていることと相似形である(林(編著)[2004]、林[2005a])。そしてその陰には、情報を事実上独占することを善と見るか、情報は共同利用することを善と見るか、というイデオロギー的対立が控えている。

しかし、この点については、より実務的な解決策を考えることもできる。つまり強い救

済を受けるためには、何らかの登録を要件とすることである。ここでの登録は、公的機関への登録に限定されない。インターネット上でアクセス可能にし、検索エンジンで検索可能にすれば、登録したと考えて良かろう。著作権について、この登録を前提にした新しい提案が私の㋡マーク[45]をはじめ多数見られるのは、このような認識が広まっていることを示している[46]。

しかしデジタル流通が一般化する現在では、なりすましや改ざんなどの不正行為に対するセキュリティ確保などを考えない方法では、万全を期すことはできない。PKI（Public Key Infrastructure）の利用による電子署名・時刻証明などを加味した、新しい登録形態を考えることが、解決の糸口になろう。そしてこの新しい仕組みでは、意外なことに「秘密」も登録可能になるはずである。

しかし、この点についてはより詳細な分析を必要とするので、情報財の経済的特性などの分析を通じて、理解を深めて行く努力を続けたいと思う（林[2001][2003]参照）。

５．個人の秘密

主体別分類の最後の、③個人に関する秘密としては、個人情報保護への関心が高まっており、一種のフィーバー状態となっている。フィーバーの中では、日頃なら誰も気にしないことが大げさに取り上げられ、過剰な対応が正当化されてしまうこともある[47]。たとえば病院で患者の名前を呼ぶと、誰さんがどのような類の病気を患っているということが明らかになるので、名前の代わりに番号で呼ぶなどの提案が実施に移されている。

もちろん、この提案もRFID(Radio Frequency Identification、無線タグとかICタグと呼ばれている)などの技術的な支援手段と結びつければ、誤りを最小限にしつつ導入が可能かも知れない。しかし、慣れ親しんでいる名前を呼ばれて間違う確率はほぼゼロと見られるのに対して、番号を呼ばれて間違う確率は、特に高齢者においては有意に高いはずである。名前を呼ぶことでプライバシーが侵害されるというが、病院内で偶然出会っただけでも同様のことは推測可能なのだから、この問題は伝統的なプライバシーとは関係ないと割り切ることもできよう。

こうした問題が紛糾する原因の一つとして、プライバシーと個人情報等の関係が明確になっていないことが挙げられる。英語では前者はprivacy、後者はpersonal dataで、両者

---

[45] ㋡マークは、アナログ時代の©マークに代わって著作物に付与する記号で、これによって少なくとも氏名表示権を守るほか、著作者が権利の存続期間を0年（直ちにパブリック・ドメイン化）、5年、10年、15年という比較的短期に設定することによって、著作物の流通と利用を円滑化しようというアイディア。私が1999年に提唱したもの（林[1999a]、[1999b]）。

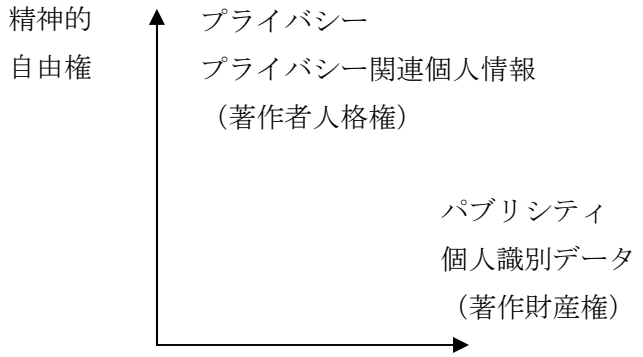
[46] ローレンス・レッシグのcc(Creativecommons)など同種の提案については、レッシグ他[2005]、林(編著)[2004]などを参照。このほか、青弓社編集部（編）[2004]、画像電子学会（編）[2005]など、これらの動向を踏まえた出版が相次いでいるのも、また一つの傾向を暗示している。

[47] 読売新聞の調査によれば、役人の天下り先の公表や、懲戒処分の対象教員名の公表を、個人情報保護法を盾に拒否している例があるという（『読売新聞』2005年8月3日朝刊トップ記事）。またより深刻なケースとしては、学校の事故で多数のけが人が幾つかの病院に運び込まれた場合に、誰がどこにいるのか把握するには相当の時間を要するという。

は明確に区別され得るはずである。ところが両者を明確に区別して出発したはずの OECD 加盟国の間も、3 つのタイプに分かれている。第 1 グループは、personal data の保護を法定したイギリスに代表される。第 2 のグループはその正反対に、プライバシー侵害を主体に成文法の範囲を限定し、残りは業界の自主規制に委ねるもので、アメリカがその代表である。その中間にあって、ヨーロッパ大陸各国では両者を区別していない。

わが国では、意識的にか無意識的にか、両者が混同される傾向がある。この差を明らかにするには、個人情報がパブリシティと同様の効果を持つと同時に、個人識別データとして経済的価値を持つ場合もあると考えて、「精神的自由権」と「経済的自由権」のマトリクスを活用することが有効であろう[48]（図表 8 参照）。

図表 8　プライバシーと個人情報



（出所）筆者作成

たとえば一般人の場合に、私生活が世間に知られていないとすれば、その平穏を守りたいという願望は「プライバシーの権利」として主張し得る（精神的自由権）。ところが有名人（celebrity）とりわけ芸能人の場合で、私生活を既に世間に広く知られている場合には、プライバシーの権利は放棄したと見てよいのではなかろうか。逆に芸能人の場合には、その写真や特徴などが商品価値を持つ限り、それらに対して「パブリシティの権利」を主張して、経済的利益を得ることはできるし、その権利が侵害された場合には、差止や損害賠償を請求できると考えるべきであろう。

最後に残る問題は、パブリシティの権利では救済が困難な場合に、「最後の拠り所」（last resort）として、プライバシーの権利に戻って救済を求めることができるか否かであるが、私見ではその余地を残しておくべきではないかと思う。というのも、プライバシー対パブリシティという局面では未だ問題が顕在化していないが、プライバシー対個人識別データという局面では国を挙げての大騒動が展開されたからである。

[48] この用語は憲法学に端を発し、基本的人権のうち「言論の自由」（憲法 21 条）などを「精神的自由権」と、「財産権の保障」（同 29 条）などを「経済的自由権」として区別し、憲法上の保護は前者に対してより厚いとする「二重の基準論」が通説となっている。

発端は住民基本台帳が全国ネットワーク化され、個人識別のための基本 4 情報（氏名、生年月日、性別、住所）が広く伝達・処理・蓄積されることが現実的になったことと、域外国との電子取引にも、個人データ保護に関する「十分なレベルの保護」(adequate level of protection)を求めたEU指令[49]により、わが国も同レベルの保護を検討せざるを得なくなったことである。そこでOECDのガイドラインにならって、民間における個人情報保護法を制定することになり、当初マス･メディアは、法制化に原則賛成していた。しかし、個人情報を広く扱う者に義務を課そうとすると、マス･メディアも必然的にこれに含まれてしまうことが判明した頃から、全くわが身可愛さの気持ちから目が曇ってしまった、と言うしかない。

加えて、住民基本台帳ネットワークのために、国民一人一人に番号を付与することが「国民総背番号」という見方につながり、感情的な反対論がマス･メディアを支配してしまった。マス･メディアを適用除外とすることは当初から政府も明言していたのに、このようなドタバタ劇のお陰で、インターネットはマス・メディアとして扱わないなどの不合理な線引きが残ることになり[50]、歴史に汚点を残すことになったのが残念である。

もし仮にマス･メディアの側に知恵者がいて、「個人識別データはプライバシーとは違う」ということを明解に説明していれば、このような大騒ぎにはならなかったであろう。上記の基本 4 情報のうち氏名は、識別情報の基本であり、公文書その他で広く使われている。偽名・匿名を使いたい（あるいは使うしかない）と思われる例外的なケース（例えば内部告発）を除けば、氏名をプライバシーだとして守る意義は少なく、これを隠しておくことに伴う不利益は、公開のリスクより遥かに大きいと思われる。

同様のことは、性別にも言えるであろう。性同一性症候群の患者や、性転換をした人々にとっては、これこそプライバシーとの主張もあり得よう。しかし一方で、男女差の識別が必要な空間（トイレ、公衆浴場など）もあるのだから、これもプライバシーだと観念するケースは例外と言うべきだろう。これに対して、住所のプライバシー性は他の 2 要素に比べれば高く、ATMの悪用事例などを見ると、生年月日がそれに次ぐと思われる。しかし、便利さを追求しようとすれば、これらを秘匿し続けることはできず、プライバシー的要素を放棄しなければ、ハイテクに対応することはできない[51]。

---

[49] 95/46/EU指令と呼ばれる「個人データ処理に係る個人の保護及び当該データの自由な移動に関するEU指令」では、その 25 条 1 項で次のように規定している。「構成国は、処理過程にある個人データまたは移動後処理することを目的とする個人データの第三国への移転は、この指令の他の規定に従って採択されたその国の規定の遵守を損なうことなく、当該第三国が十分なレベルの保護(adequate level of protection)を確保している場合に限って行なうことができるということを規定しなければならない」(堀部[1997]訳による)。

[50] 「個人情報保護法」50 条によれば、「放送機関、新聞社、通信社その他の報道機関（報道を業として行う個人を含む。)」が「報道の用に供する目的」で（同条 1 項 1 号)、「著述を業として行う者」が「著述の用に供する目的」で（同 2 号）個人情報を扱う場合には、個人情報取扱事業者に当たる場合であっても、適用除外とされる。しかしここでは、出版業者やインターネット接続業者(ISP=Internet Service Provider)は、明示的には含まれていない。

[51] もっとも、このように述べたからと言って、現在の住民基本台帳法が基本 4 情報を公開情報とし、しかも開示請求者の身元も確認していないことを肯定するつもりはない。本文に述べたように基本 4 情報の扱

とすると、個人情報の出自はプライバシーにあるかもしれないが、それは言わば精神的自由権としては放棄され、専ら社会生活を営む上で欠かせない識別子として（経済的に）使われているのが、個人識別データだという見方ができよう（この点を明らかにするためには、個人識別データという無味乾燥な用語のほうが良いかと思う[52]）。つまり前出のプライバシー対パブリシティという関係のコロラリーとして、プライバシー関連個人情報対個人識別データという図式を考えることができるのである。

このように考えるヒントは、著作権制度にある。周知のように著作権は多くの権利（支分権）を束ねたものであるが、大別して著作者人格権と著作財産権に分けられる。通常の経済行為を行なう限りでは後者だけを考えておけばよいが、ごく例外的なケースでは人格権が問題になることがある。例えば、ロール・プレイング・ゲームの筋書きを無効にしてしまうようなソフトが問題になったケース（ときめきメモリアル事件[53]）では、人格権が脚光を浴びている。

この点に関し、個人情報を人格権的利益―経済的利益、社会的開示―秘匿という 2 つの軸で分類し、その座標軸の移動を論ずる船越[2001]の視点は示唆に富んでいる。即ち「小集団社会では個人識別データの経済的価値が特に大きかったわけではない。それが電子商取引の時代では、個人情報集積の第一の基礎となるため、経済的価値が高くなる方向に位相が移動したのだと考えられる」として、次のように言う（図表 9 参照）。

「実線で示した縦軸横軸が交差するところを原点 a とすると、原点 a による個人情報の位相は、サイバースペース以前の状態を示している。伝統的プライバシー権のうち私生活の平穏権は主として[Ⅱ]の領域に位置するが、パブリシティ権・有名人の氏名権は、当初から対極の[Ⅲ]の領域に位置してきたと考えられ、相互のポジショニングが示すように、極めて対照的で性質の異なる権利である。収入・負債・資産状況などは、その人のプライドともかかわるから、[Ⅳ]の領域だけでなく、[Ⅲ]の領域にも位置してきた。

プライバシー権が提唱された 19 世紀末から暫くの間、実線の縦軸・横軸が交差する位置にあった原点 a が、20 世紀後半の急激な社会構造･経済構造の変化、特にサイバースペースの出現によって破線が交差する原点 b の方向にベクトル移動したと捉えることが可能である」（船越[2001] p. 150）。

したがって、これまで主として[Ⅱ]の領域に存在したセンシティブ情報(健康状況・前科前歴等)のかなりの部分が、社会的開示と経済的利益に囲まれた[Ⅲ]の領域に存在するようになったと考えられる。こうして「センシティブ情報を含む個人情報の収集・利用が図られ、正確で最新な個人データの活用が社会的経済的に大きな意味を持つようになった、サイバースペース時代の姿が浮かび上がってくる」（p. 151）。この位相変化こそが、プライバ

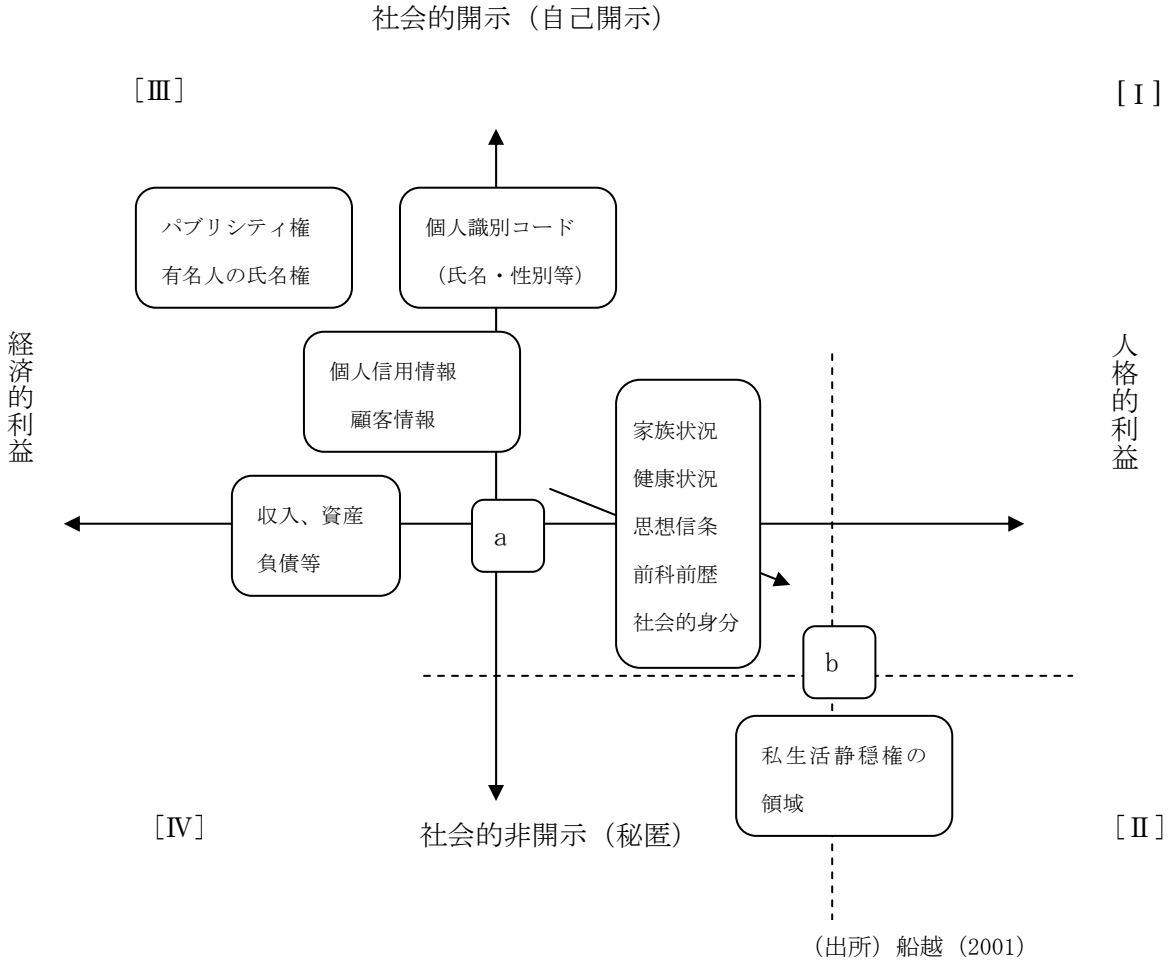
いに差を設け、それに対応して開示請求者を限定することは、当然検討すべきであろう。

52 もちろん現行の「個人情報保護法」も、個人情報、個人データ、保有個人データという明確な区分を採用している（同法 2 条、15-19 条、19-23 条、24-27 条などを参照）。しかしこれらのうち最も広義の概念を個人情報と命名してしまったため、立法者は混乱の責任の一部を負わねばなるまい。

53 最三小判 2001 年 2 月 13 日判時 174 号 78 頁。

シー権をはじめとする様々な法的秩序に影響を及ぼしているのである。

図表 9　個人情報と位相概念図

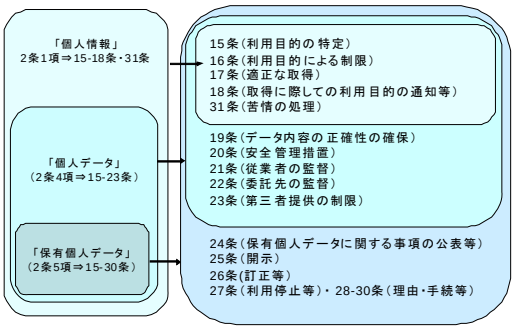


（出所）船越（2001）

このように個人情報は、何らかの形でプライバシーと結びつく要素をもっており、経済的権利と一律に割り切ることができないところに難しさがある。このことは、前 4 節で述べた「営業秘密としての顧客情報」と「個人情報保護法における個人情報」を比較して、図表 10 のような対比表を作ってみるとより明確になろう。

この図表 10 から、顧客情報が①プライバシー的要素を除外して、純粋経済財として扱われ、②保有主体は企業であり、③企業の資産の一種として保護されるには何が必要か（前述の有用・非公知、秘密管理性の 3 要件）が論じられていること。これと対称的に個人情報の場合には、①経済的自由権としての割り切りができず、精神的要素を残しており、②保有主体は個人情報取扱事業者（主として企業）であるが、権利主体は個人であり、③事業者は管理義務を課されるのみで権利が明確でない、といった傾向を読み取ることができる。

図表 10　「(営業秘密としての) 顧客情報」と「個人情報」

区分	顧客情報	個人情報
定義と根拠法	秘密として管理されている・・販売方法その他の事業活動に有用な・・営業上の情報であって、公然と知られていないもの(不正競争防止法2条4項)	生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの(他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む)(個人情報保護法2条1項)
違反行為	事業者が公正な競争を阻害する以下の行為 ①不正取得行為(同法2条1項4号) ②不正取得行為介在後の取得、または使用・開示する行為(除軽過失)(同5号) ③取得後に不正取得行為介在を知りつつ使用・開示する行為(除軽過失)(同6条) ④保有者から正当に示された後、不正目的で使用・開示する行為(同7条) ⑤不正開示行為またはそれが介在すると知りつつ、取得または使用・開示する行為(除軽過失)(同8号) ⑥取得後に不正開示行為またはそれが介在すると知りつつ、使用・開示する行為(除軽過失)(同9号)	個人情報取扱事業者(過去6ヵ月内に5000件以上の個人データの入った個人情報データベース等を事業の用に供した者)  図の出典:岡村・鈴木[2005]
救済措置と根拠法	営業上の利益を侵害された(又はそのおそれがある)者は次の救済が受けられる ①差止請求(同法3条) ②損害賠償請求(同4条)(損害額の推定がある一同5条) ③信用回復措置請求(同7条) ④刑事罰(親告罪)(同法14条)	上記の手順違反に関して主務大臣から発出される命令に違反する行為等に対して刑事罰、過料(同法56条～59条)

(出所) 筆者作成

これは企業の利益と個人の利益とが応々にして相反することから、やむを得ない差との見方もあろう。しかし①の差は、個人情報保護基本法という形で立法がなされ、細部は業法等に委ねられていれば緩和されていたかも知れない。②と③について産業界や学界には、現行法の間接罰方式[54]では効果がなく、直罰方式すなわち「情報漏洩罪」を新設すべきだとの意見もある (古くは西田[1998]、最近では堀部[2004])。自由民主党は、個人情報保護法を修正して、「個人情報漏洩罪」を新設する方向で検討中といわれる。

しかし特別法による場合も、犯罪の客体である「個人情報」あるいは「個人データ」の概念を明確にしなければならない。ましてや、「個人情報」を越えて広く「情報漏洩」を一般法である刑法で検討するのであれば、「情報」や「漏洩」の構成要件を厳密に論じなければならない。規定の仕方如何では、「本の立ち読み」が犯罪に該当する恐れさえあるからである。

ここで、一部の論者が強く主張するように、個人情報保護法が「自己情報コントロール権を確立した」とするのは、偏った見方であることだけは留意しておきたい。なるほど今日のような情報化が進んだ状況では、プライバシーの権利を「一人で放っておいてもらう

[54] 「個人情報保護法」で個人情報取扱事業者の行為が直ちに処罰の対象になるのではなく、主務大臣の勧告や命令が発せられ、それに違反したときにはじめて罰せられる (同法 34 条、56 条) ので、このように呼ばれる。

(to be let alone) 権利」と考えるのは狭すぎるかも知れない[55]。しかし「自己情報をコントロールする権利」と前広に解釈すると、精神的自由権の側面を強調しすぎることになろう。図表 10 が示すのは、経済的自由権を主としつつ、精神的自由権の要素を残している、現在の「個人情報」の姿であろうかと思われる。

ところでこのような現代のプライバシー問題を考えるにあたっては、憲法論争のような実体論議をすることも大切だが、手続き論からも意外に有益な示唆が得られる場合がある。ここで有名なのが、opt-in と opt-out の差である。opt-in とは、ある条件の取り扱いについて、事前に該当者の同意を必要とする仕組みで、反対に opt-out とは事前の同意を必要としないが、該当者が取り扱いに不満ならその契約を事後的に解除する自由を持つという仕組みである。個人情報に限って言えば、情報の収集や利用に、事後的に個人情報の削除を求め得るのが opt-out ということになる。

そして、プライバシー関連個人情報と個人識別データを分けて考える私の立場からすれば、opt-out が保障されてさえいれば、個人情報を自由に扱ってよいこととしなければ、e-commerce などの商行為が著しくやりにくくなるのではないかと考える。従って一般的には opt-out で十分としておき、本来のプライバシーにまで戻って議論すべきような、著しい不都合が生じた場合に限って、精神的自由権の発動を留保しておきさえすればよいと思う。

ただし、e コマースの運用の実態からは、次のような指摘もある。opt-out の通知をすることは、私が現に存在し、先のメールを間違いなく受け取ったという「存在証明」になってしまう。従って、受け取りたくないメールなどを排除するには効果が無く、黙殺するかアドレスを変えるなど他の方法によるしかないのだと。この難題に対処する方法は、今のところ見出されていない。

５．秘密保護の一般法

ここまできたら、主体別に秘密の保護を論ずるのではなく、一般の法律において秘密（あるいは情報）がどのように保護されているか（あるいは、いないか）を論ずる時期だろう。まず民事法から見ていこう。

有形財を中心とする民事法体系の根幹は、時代の変化にもかかわらず、ほとんど変化していない。民法[56] 85 条において「本法において物とは有体物をいう」とあるのが象徴的である[57]。そしてそれには、十分な理由がある。有形財の場合には、「自己のためにする意思

[55] プライバシーの権利を初めて論じた論文とされるWarren and Brandeis[1890]では、このように定義していた。それに対して、コンピュータとネットワークが急速に発達した現在では、「自分の情報は自分でコントロールする権利があってしかるべきだ」とする説が抬頭するのは理解できる。しかし情報の本質を理解すれば、それがコントロール不能であることは明らかだろう。

[56] 「民法」（第 1 編～第 3 編は、1896 年法律第 89 号）。

[57] 70 年代以降わが国でも、ソフトフェアを特許法によって保護するようになったが、「発明」の 3 分類（物、方法、物を生産する方法）のうち「物」として位置づけた（特許法 2 条 3 項 1 号）ところにも、有体物中

をもって物を所持する」ことが可能で、法的にはこの「占有」（民法 180 条）を前提に、権利者の排他権を認めたものが「所有権」であり（民法 206 条)、これを（第三者を含む）社会一般に担保する仕組みが、不動産の登記や動産の引渡などの「対抗要件」である（民法 177 条、178 条など)。

ところが「情報財」は、本人でさえ触って確認することができない実体のないものだから、他人の使用を排除することはきわめて難しい。また誰かに「情報財」を引き渡したつもりでも、私の手元には同じものが残っている。つまり法的には「占有」状態が不明確だし、明確な移転も起こらないのである（中山[1995]、併せて林（編著）[2004]、林[2005a]参照)。

もっとも「情報の保護」と真正面から銘打たなくても、実行上これに近い効果を与えてくれる規定は存在する。たとえば民法の「不法行為」（709 条以下）においては「他人の身体､自由又は名誉を害したる場合」に「財産以外の損害に対しても」損害賠償の責任を課している（710 条）から､秘密の暴露など「非財産的損害」も保護されていることになる。

しかし不法行為によって事後的に救護される場合（一般不法行為規制、アメリカ法では Liability Rule）よりも、事前に排他権が与えられていて他人の利用や妨害を排除できる場合（権利付与法制 Property Rule）の方が保護の程度が強いことは明らかである。知的財産制度はこの後者の代表例と言える（Calabresi & Memaled [1972])。この中間に、不正競争防止法などによる保護があるが、これは競業者間という狭い範囲にしか適用されない。この 3 者の関係を表示すれば、図表 11 のようになる。

図表 11　知的財産の保護方式

方式	内　容	現行法	効　力
権利付与	創作者に権利を付与する	特許法 著作権法など	妨害排除、損害賠償請求、譲渡、相続、実施許諾、第三者への対抗、担保権の設定など
特定行為規制	不正競争により創作権等営業上の利益を害する行為を禁止する	不正競争防止法	差止請求，損害賠償請求， （損害額の推定の規定あり）
一般不法行為規制	故意または過失により、創作者等の利益を害する行為を禁止する	民法	損害賠償請求のみ

（出所）筆者作成

このように考えてくると､改めて「所有権」が極めて強い排他権であることが確認できよう。所有権は表 3 の権利付与方式の「効力」欄に掲げるすべての機能を有している。また

心の発想が現れている。しかも当初は、プログラムが媒体に記録されていることを要件としてきたが、2000 年末からは記録されていない場合も「物の発明」であるとした。後述の「著作権は所有権とは違う」という記述と対比せよ。

所有権に代表される財産権（＝物権）は民法に特定されていて、「財産権はこれを侵してはならない」と憲法に明記されている（29 条 1 項。ただし例外はあるが)。20 世紀の冷戦構造が崩壊したのは、結局のところ私的所有を前提にした資本主義システムの方が、経済社会を律する方法として適していたことになろうか（ただし、その勝れていたはずのシステムが資源浪費を抑制できなければ、環境問題を解決できずに崩壊するかも知れないが)。

このような所有権の特徴を知ってか知らずか、知的所有権という用語が使われることがあるが､情報が所有の対象になり得ないことは繰り返すまでもないだろう。この問題は一見言葉の問題のように見えるが、実は権利の強弱をどう捉えるかに関係している。そして、公的機関に対する出願・審査や登録を要件とする特許権の場合（特許法 36 条、47 条以下、66 条など）より、何らの手続きを必要としない（無方式主義の）著作権の場合（著作権法 17 条 2 項）に、より先鋭な形を取る。

「モノ」を中心とする近代社会が、所有権という法システムによって支えられ発展してきたとすれば、情報化社会においては「情報」に関する新しい法律の構築が求められている、と言えよう（升田[2003])。また、このことは実体法のみならず手続法の分野にも（あるいは手続法の分野には、より強く）妥当すると見るべきかも知れない（安富[2000])。

一方、刑事法の分野はどうだろうか。刑法[58]は社会秩序の安定のために、国家が一定の行為類型を犯罪と特定し、それに対して相応の罰を課すための基本法である。民事法におけるほど明確ではないにせよ、ここで保護されるべき法益としては、まず有形財が念頭に置かれてきたことは間違いない[59]。

例えば窃盗罪は「他人の財物の窃取」が要件である（刑法 235 条）が、ここで財物とは有形のものであった。しかし既に戦前において、裁判所は「電気」窃盗に窃盗罪を適用し、戦後はこれを明確にするため､窃盗および強盗の章においては「電気は財物とみなす」旨の規定（刑法 245 条）がおかれている。「みなす」ということは、「A ということと、元来性質の違う B ということを､ある法律関係では同一に見る」という意味だから（林 (修) [1975])、反対解釈をすれば、刑法は「体化された情報」の例外として無形財の電気のみを保護し、情報窃盗は対象にしていないと言える。

しかし他方で少なくとも見かけ上は、有形物に体化されない情報そのものが、保護されているかに見える条文もある。たとえば秘密漏示罪（刑法 134 条）は､医師や弁護士､公証人などの者が､業務上知り得た他人の秘密を漏らすという行為を処罰するので、一見直接「秘密」を保護しているように考えられる。しかし通説の立場では、保護対象はたとえば依頼人の弁護士（司法制度）に対する信頼感であり、一般人の一定の職業に対する信頼感を保護することによって､その反射的効果として「秘密」が保護されているに過ぎない。

またコンピュータ化の進展につれて、これを利用した犯罪が多発したため､1987 年の刑法改正において「電磁的記録不正作出・供用罪」（刑法 161 条の 2）や「電子計算機損壊等業

58 「刑法」(1907 年法律第 45 号)。

59 ここではむしろ 1991 年という早い時期から、企業秘密やコンピュータ・データの刑事法的保護のあり方に注目してきた、佐久間[1991][2003]の先駆性が目立っている。

務妨害罪」（刑法 234 条の 2）などの罪が、2001 年には「支払用カード電磁的記録に関する罪」の章（刑法 18 章の 2）が新設･追加された。これらの場合の保護対象は「電磁的記録」（刑法 7 条の 2）であるが、これまたデータそのものではなく、有体物に体化されたものと位置付けられていることに注意すべきである。したがって総じて言えば、刑事法は「秘密」のような無形のものを直接保護する態度は取っていない。

ただし、2001 年の刑法改正によって、「支払い用カード電磁的記録不正作出準備罪」（刑法 163 条の 4）が新設され、支払い用カード電磁的記録不正作出等のために「電磁的記録の情報を取得した者」も刑事罰の対象になった。これは「情報そのもの」を犯罪行為の客体と定めた最初の例であるとも言え（佐伯[2002]）、今後の参照例となろう。

これに対して、財産上の価値のある情報（財貨としての情報）については､いわゆる 2 項犯罪（強盗罪・詐欺罪・恐喝罪の各 2 項）として「財産上不法の利益」が客体とされている(刑法 236 条、246 条、249 条各 2 項)。通常は､債権の取得や債務の免脱、債務履行期限の延期などが該当するであろうが､情報を欺網･暴行･脅迫などの方法で取得した場合には、情報それ自体が 2 項犯罪の保護対象となり得る。

無形のデジタル情報が保護ないしは処罰の対象であるが否かが、深刻な問題を提起しているケースとして､情報窃盗がある。前述した通り電気窃盗が立法論的に解決された今日では､反対解釈として「情報は財物ではない」として、窃盗の構成要件に該当しないと見るしかあるまい。顧客情報の流失や盗用を秘密侵害罪として処罰する先進国がみられるものの、わが国の秘密漏示罪は前述の通り犯罪行為の主体を限定しており、「実質秘」性を具備しない電気信号の集積や公開情報を編集したプログラム及びデータベースは、同罪における「秘密」に含まれないことが多い[60]。確かに「有体物」でなくても安易に窃盗や横領の対象とされるようであれば、「カンニングや本屋での立ち読みも窃盗罪になってしまう。奪取罪である窃盗罪には､やはり行為客体の有体性の要件は無視できない」(園田[1999]) とするのが、解釈学の限界であろう。

このように秘密そのものを法的客体としてどう守るかではなく、1 での述べた情報の生産・保管・流通・消費の過程において情報（その中には秘密が含まれよう）へのアクセスを規律する法律として、不正アクセス禁止法[61]がある。

この法律制定前は、データなどの改ざん・抹消を伴う不正アクセス行為は、電子計算機損壊等業務妨害罪（刑法 234 条の 2）の対象となりうるが、改ざんなどを伴わない単純な不正アクセス行為は、処罰の対象外であった。しかしコンピュータ・ネットワークを活用し

---

[60] またコンピュータ・プログラムは 1986 年から「著作物」とされることになったが（著作権法 2 条 1 項 10 号の 2)、法改正以前の事件として新潟鉄工事件（東京高判 1985 年 12 月 4 日、判時 1190 号 143 頁）がある。同社社員であった被告は、自分が職務上作成したシステムを外販しよう主張したが容れられず、別会社を設立することにした。その際、同僚と共にシステム設計書等一式を社外に持ち出した行為が業務上横領罪（刑法 253 条）に問われた。被告は、著作権は自分に帰属するので、正当なコピーだと主張したが、容れられなかった。この事件には多数の複雑な論点が含まれているが、ここでの問題は、有体物の横領という刑事事件として裁かれていることである。

[61] 「不正アクセス行為の禁止等に関する法律」(1999 年法律第 128 号)。

た、いわゆるハイテク犯罪は増加の一途をたどり、その社会的影響力や未成年者による実行などが社会問題となった。そこで不正アクセス行為を一般的に禁止する法律として不正アクセス禁止法が制定・施行され（2000 年)、上述の単純な不正アクセス行為や、パスワード屋のような不正アクセス助長行為も処罰対象となった結果、機密性がより強く保護されるようになった[62]。

この法律には、今後コンピュータ通信基本法とでも呼ぶべき役割が期待されよう。しかし、電気通信を所掌する総務省（旧郵政省）は、この法律が警察庁・経済産業省との共管であり、かつ主務官庁ではないことから、私の理解のような位置づけをしていないのが残念である[63]。

この法律の体系は、「不正アクセス行為の禁止・処罰」と「防御側の対策」の二部構成になっており、前述の営業秘密におけると同様、管理側の義務も明記されている点が特徴的である。まず前者としては、

① 不正アクセス行為に関して禁止行為（3 条）と罰則（8 条）を定め、
② 他人の識別番号の無断提供の禁止行為（4 条）と罰則（９条）
を規定している。

後者としては、

③ アクセス管理者による防御措置として「識別符号等の漏洩禁止」「アクセス制御機能の高度化」が義務づけられている（5 条）ほか、
④ 都道府県の公安委員会による援助（6 条）や、
⑤ 国家公安委員会、経済産業大臣、総務大臣による、情報提供等（7 条)、
が規定されている。

しかし、⑤項による情報提供は行なわれているものの、ここに報告される事例は「氷山の一角」との感は否めない。これは、もともと官に期待することに無理がある（下手をすれば検閲につながる惧れがある）ことに加えて、民の側の隠蔽体質にも問題がある。既にマス・メディア等によって事件が公になっている場合には、自社の毅然とした態度を示すべくマスコミ対応したり、刑事告訴に踏み切るケースもある。しかし、事が公になっていない場合には、なるべく隠し通してしまおうという態度も見られるという（岡村[2003])。

事案にもよるが、事実をありのままに発表することが信頼を勝ち得ることが多いのは、内部告発などと共通しており、これが「ネット告発」の場合には、尚更である（ネットワーク・セキュリティ研究会[2003])。先に「秘密は公開して守る」というパラドクスが存在

---

[62] なお、改ざんなどを伴った不正アクセス行為や、サーバへの侵入を伴わないサービス妨害攻撃も、電子計算機損壊等業務妨害罪の対象となりうる。これはサーバに過負荷をかけたり、ソフトウェアのバグを狙うなどの方法によって、標的となるサーバの運用を不能にする攻撃方法であり、「DoS攻撃（Denial of Service attack)」とも呼ばれている。

[63] 旧郵政省が実質的に監修している『情報通信法令集』(情報通信法制研究会（2004)）は、この分野の法令を、①行政通則 ②有線電気通信 ③電波 ④電気通信事業 ⑤放送 ⑥IT社会構築 ⑦振興・技術開発 ⑧関係機関 ⑨その他、に分類しているが「不正アクセス禁止法」は⑥のIT社会構築に位置づけられている。理論的には望ましい分類ともいえるが、官僚の弊として①～⑨の順位が、力の入れ方と相関しているようで気にかかる。

し得ることに触れ（第 1 節)、知的財産制度はその具体例であるとも述べたが（第 4 節)、内部告発への対策では、公開すべき情報と秘匿すべき情報の峻別が、求められていると言えようか（注 11 を併せて参照)。

また、不正アクセスに関する情報を被害者間で共有し、対策に生かすことが求められている。いわゆる ISAC(Information Sharing and Analysis Center)の動きなど、この分野ではアメリカに学ぶべき点が多い。たとえば司法取引の制度などは、公平を旨とするわが国の法文化では「とんでもない」と言われそうだが、人間に 100%があり得ず、「いつ間違ってもおかしくない」存在である以上（Kohn et al.[2000])、事件・事故の真相解明のためには、不可欠の制度のように思われる（村上[1998])。

総じて言えば、これまでのわが国の法制度や慣行は「お上の指示待ち」の傾向が強かったが、今後は民主導で自発的に対策を実施し、官には最低限の法整備を期待する、といった態度が必要となろう（ここでの民には、NPO などが当然含まれる)。ドッグ・イヤーで変化する情勢には新しい対応が必要で、不正アクセス禁止法の主眼は、上記①と②にあると言えよう。

ところで、秘密の保持に関しては、一般法における漏洩の禁止規定よりも、個別法あるいは業法における諸規定の方が、より実効性を担保していることにも、注意を喚起しておこう。たとえば 2 で述べた公務員の秘密を守る義務や、3 で述べた通信事業者の秘密保持義務はその代表例である。それ以外にも、前述の医師・弁護士など、それぞれの業法に義務規定があり、公認会計士は公認会計士法に罰則規定がある（ただし親告罪)。また各種の公的調査と守秘義務の関係（刑訴法 197 条 2 項、弁護士法 23 条の 2 など）など、行政が係る行為についての守秘義務は幅広く規定されている。

６．契約による秘密の保護：営業秘密の場合

前節で述べたように、現在の制定法は秘密を真正面から見据え、これを保護するための手段を十分に整備しているとは言い難い。また現在の不正競争防止法には、営業秘密の保護を直接の目的とした民事・刑事の規定が置かれているが、企業取引の中で秘密として管理することが求められる場面はさまざまであり、法律による一律の規制だけでは、必ずしも十分ではない。となると秘密を保護したい人々は、契約を活用していこうとするのが自然の流れである。とりわけ商取引においては、取引の安全性が決め手であるから、守秘義務契約・競業禁止契約などが一般化している。

営業秘密の開示および使用を直接的に禁止する「秘密保持契約」さえあれば、秘密保持のためには必要・十分のようにも見える。このような契約は「契約自由の原則」により一般的に有効とされているからである。しかし、契約の内容がいくら自由であったとしても、そのエンフォースメントは実際にはかなり難しい。営業秘密が他の企業によって現実に利用されたか否かを確かめ、証明することが、ディスカバリ[64]のような証拠収集手続きを欠く

[64] ディスカバリとは、英米の裁判手続きにおける情報開示制度で、正式の審理に先立って訴訟当事者双方

わが国では困難なためである。そこで、予防的な手段として、従業員・役員や取引先等との間で、「競業禁止契約」が利用される（小塚[2004]）。

しかし、競業禁止契約は競争者の出現を阻止し、現状の取引関係を維持するという目的で利用されることもあり、文字通りの効果を認めると過剰な規制になりやすい。したがって秘密保持契約とは異なり、無条件で「契約の自由」を認めるわけにはいかないと考えられている。すると問題は、いかなる根拠で、いかなる限度の競業禁止契約が有効であるか、ということになる[65]。

従業員（被傭者）が、労働契約の継続中に秘密保持義務及び競業避止義務を負うことは、異論なく認められている。これに対して労働契約終了後（退職後）これらの義務が肯定されるか否かは、従来から議論の対象とされてきた。現在の支配的な学説は、①秘密保持義務が一定の範囲で肯定されるべきことは1990年の不正競争防止法改正により明確になったが、②競業避止義務は明示の特約がなければ認められず、③競業禁止が明示的に合意されている場合であっても、「それは禁止の対象となる期間、地域、及び行為の種類が合理的な範囲に限定され、かつ代償が与えられていることを要件とする、と解している」（小塚[2004]）。

裁判例では、競業それ自体の差止が求められるよりも、特約に反する独立や引き抜き行為に対して不法行為責任が追及されることが少なくない。しかしこうした裁判例も、退職後の競業禁止契約は従業員の職業選択の自由と緊張関係に立ち、したがって文字通りの効力を認められるとは限らないという基本的な考え方においては、学説と一致している[66]。

企業が守ろうとする営業秘密は、具体的には従業員やそのグループ、あるいは代理店によって開発されたものであろう。とすると、その情報は企業と従業員のいずれのものかという問題に直面する。たとえば従業員や代理店が顧客を開拓した場合、現実にその顧客と接しているのは従業員ないし代理店であるが、事業者の指揮命令下で、またはそのビジネス・モデルの下で、事業者のブランドと資金を利用して営業がなされることが多いので、従業員等は事業者の補助者にすぎないとも言える。

ここで「従業員（代理店）のもの」とされる情報の範囲が大きいほど、従業員（代理店）が情報を開発するインセンティブは高くなるが、そうした情報の開発を促すような投資を行なう事業者のインセンティブは低くなる。この両者を総合して見たとき、開発された情報のうちどこまでを「従業員（代理店）のもの」と認めれば最も大きな効果が収められるかは、個々の企業やそれを取り巻く環境によって異なると思われる。

が、事件に関する証拠と情報をお互いに開示すること。当事者が裁判所に罰則付き召喚状(subpoena)を発行してもらい、証人に情報の開示を求めることもできる。

[65] これに対して、事業者間取引（たとえばフランチャイズ契約）に伴う競業禁止契約については、主として競争法の観点から若干の議論がなされるにとどまり、「両分野を一貫した検討は、なお不十分であるように感じられる」（小塚[2004]）。この問題に関するわが国の裁判例は、従来、もっぱら労働者と雇用主との間の契約の事例において現われ、労働法の分野で多く論じられてきた。

[66] これに対して事業者間契約の場合には、契約終了後の競業禁止契約に、より強い効力が認められるようにも見えるが、ここでは深入りしない。

従来の学説は、従業員が雇用期間中に取得する知識・経験を一般的なものとその企業に独特なものとに分け、事業者に属するのは後者のみであるとしてきた。しかしそれは、個別企業の事情に通じた当事者が、最もよく判断し得る問題だと考えられる。一般的な知識・経験と企業に特有なものに分ける見方は、当事者が選択するであろう契約の内容を、一般化して記述したものと見ることもできよう。

企業にとっては、自社で開発したノウハウを秘密管理することにより、競争者に対して優位な地位に立てるという事実が、より良き商品・サービスを提供するインセンティブとして機能し得る。そうだとすれば、従業員の転職により、情報・ノウハウの流出を放置すれば、成果開発のインセンティブとしての秘密管理の機能を失うことになる。

他方、より高い評価を与えてくれるとか、能力を如何なく発揮できるとか、あるいは企業の風土が性分に合っているとか、さまざまな意味で自分にとってより有利な職場環境で就業したいという労働者の利益は、最大限に尊重されてしかるべきである。労働という機会を活用して自己実現を図るという、単なる経済的な自由に止まらない価値を見出すことができるからである。競業禁止協定の有効性は、この両者のバランスの上で解釈されなければならない。

これらの点に関して、実務上の指針となり得るのが、後述する「営業秘密管理指針」である。そこでは、この節で述べてきた一般論を記述することに加え、①秘密保持契約の内容、②契約のタイミングと事務手続き、③企業間の秘密保持契約との関係などについて、「かゆいところに手が届く」ような懇切な解説が加えられている。

このうち最も包括的な①の内容について細部を見ると、ⓐ対象となる情報の範囲、ⓑ秘密保持義務および付随義務、ⓒ例外規定、ⓓ秘密保持期間、ⓔ義務違反の際の措置等について、判例の動向も踏まえて解説している。これらは実務家にとって、きわめて有益な解釈源となり得るであろう。

7．秘密の管理方法と救済レベル

2005 年 4 月の個人情報保護法の本格施行を契機として、企業の取り扱う個人情報の管理の重要性が認識され、その手段として情報セキュリティ・マネジメント・システム（ISMS）[67]の役割が強調されるようになった。一方多くの企業は、競争環境において自らの比較優位を保つために、新技術・製品に関するノウハウや顧客情報等を、企業秘密として管理している。これらの秘密情報は、不正競争防止法において知的財産権の一つである「営業秘密」として保護されている。

このように目的は異なるとはいえ、顧客リスト・従業員リスト等の情報は、個人情報保護の対象であると同時に企業秘密ともなり得る。したがって、企業運営を合理的に行なうためには、個人情報保護のための秘匿性確保と営業秘密の保護のための秘密管理との対策

[67] ISMSとは、国際基準に則り、情報セキュリティの一定レベルを達成していることを第三者機関が認証する仕組み。わが国では、日本情報処理開発協会（JIPDEC）がその運用に当り、適合性評価基準として「ISMS認証基準」（Ver.2.0，2003 年 4 月改訂）を定めている。

を、できるだけ共通化することが望ましい。個人情報保護法に基づく秘匿性確保の適否に関する判例は存在しないが、不正競争防止法に基づく秘密管理性の有無に関する判例は多数存在するので、前者の予測をするためにも、後者を分析することが有意義と考えられる（苗村[2005]）[68]。

2003 年に策定され、現在改訂作業中の経済産業省「営業秘密管理指針」は、その第 3 章で秘密管理性を確保するための方法を示している。まず秘密管理性を判断した 49 件の判例中、秘密管理性を肯定したものは 14 件であるが、それらの判例[69]は、アクセス制限（情報にアクセスした者を特定すること）と客観的認識可能性（情報にアクセスした者が秘密であると認識できること）の基準の下、個々具体的に秘密管理性を判断している[70]として、次の要素を挙げている。

1. 物理的・技術的管理
   (1) 基本的な考え方
   (2) 物理的管理
   (3) 技術的管理
2. 人的管理
   (1) 基本的な考え方
   (2) 従業者に対する教育・研修の実施
   (3) 従業者、退職者等に関する就業規則・契約等による秘密保持の要請
   (4) 派遣従業者
   (5) 転入者
   (6) 取引先
3. 企業と従業者・退職者との適切な秘密保持契約の在り方
   (1) 秘密保持契約を締結する意義
   (2) 秘密保持契約の内容
   (3) 秘密保持契約を締結するタイミングと事務手続き
   (4) 企業間の秘密保持契約との関係
4. 組織的管理
   (1) 自社の営業秘密管理のための組織的管理
   (2) 他社の営業秘密を侵害しないための組織的管理
   (3) 望ましい管理方法
   (4) 情報管理に関するマネジメント規格、個人情報保護との関係

そしてこれらの記述の中で、しばしば「情報セキュリティ・マネジメント・システム

[68] ただしこのことは両者を同一視したり、混同することと同じではない。次に述べる「営業秘密管理指針」ではむしろ両者を「峻別することが望ましい」としている。
[69] たとえば東京地判 2000 年 9 月 28 日。平成 8 年(ワ)第 15112 号。
[70] この点は第 4 節で述べたところと変わらない（千葉大IP研究会[2005]および青山[2005]）。

（ISMS)」の手順に触れていることが印象的で、前述の苗村[2005]の指摘の正しさを裏付けている[71]。既に数ヵ所で触れたように、「秘密」は情報の一種であるから、放置すれば自然に拡散し、秘密でなくなる可能性が高い。そこで保有主体があくまでも秘密として保護してもらいたいのであれば、相応の管理義務を負うことになる。

有形財の取引を中心とした世界でも、いわゆる「善良なる管理者の注意義務」（善管注意義務）が必要とされ、これを全うしないと過失となり債務不履行の責任を問われることがある(民法 400 条における特定物引渡しまでの義務､同 644 条における受任者の義務など)。この善管注意義務のレベルはというと、「当該事情のもとで取引上客観的に要求される」もので「通常人ならば注意することができたという場合には、たとえ具体的行為者の注意能力では努力しても注意できなかったとしても善管注意義務違反が認められる」（國井・三井[2001])。

これに対して「自己の財産におけると同一の注意義務」は、行為者自身の注意能力に照らして注意を尽くしていれば、たとえ通常人ならば注意することができたと認められる場合でも、注意義務違反にならない。寄託契約における無償受託者の義務（民法 659）の場合がこれで、親権者の注意義務（民法 827 条）や相続の限定継承者の義務（民法 926 条 1 項）なども、表現に微妙な違いがあるが同レベルの注意義務だと解されている。つまり「自己の財産におけると同一の注意義務」は、善管注意義務よりも低いレベルにある。

これらに対して、秘密の管理義務はいくつかの点で違いがある。

①まずレベル的には、秘密管理義務が善管注意義務より高い（しかも、かなり高い）と考えられる。これを直接的に示す条文はないが、後述するような標準やガイドライン等に定められた手順は高度なもので、これを守っていくには相当の努力が必要である。前述したように、個人情報保護法（およびそのガイドライン）をめぐって過剰反応とも言える保護強化への流れが生じたのも、このレベルの高さが影響している面は否定できない。

②次に義務違反の効果について。民法上の一般原則は、それによって過失責任を問われる場合がある、というものであった。秘密管理義務についても同様の効果を生じるものがある（たとえば個人情報保護法 20 条)。しかし逆に、秘密管理性が秘密保護の要件になっているに過ぎず、これを怠っても権利を失うだけで法的な責任は生じないもの（たとえば不正競争防止法 2 条 4 項）もある。前者を義務違反型、後者を権利喪失型と呼んでおこう。

③民法の一般原則である善管注意義務は、抽象的な概念であって、裁判においてその具体的含意が絞り込まれることはあっても、その手順をマニュアル化しようという発想とは無縁である。これに対して秘密管理義務は、ISMS 等の手順として標準化・ガイドライン化・マニュアル化されている。というよりむしろ、技術情報に関する標準化の動き全体の中にセキュリティの要素が取り込まれ、手順書が出来上がったと言った方が史実に近

[71] ただし、既に個人情報保護に関して述べたとおり、営業秘密としての顧客情報の保護手順と、個人情報保護の手順を峻別せよとしている点が、かえって際立っている。

い。ここには文系的発想と、理系的発想の違いが見られる。

それでは、秘密管理における管理レベルと、それが破られた場合の法的救済のレベルとは、どのような関係にあるのだろうか。また、そもそも管理レベルとは一時点で固定可能なものだろうか。ここでも幾つか、特徴的な点を挙げることができる。

①ISMS 等に定められた手順には、すべて忠実に守られることを期待した「ミニマムの水準（以下 ML=Minimum Level）と、いわば理想型である「望ましい水準」（以下 BP=Best Practice）とがあり、これらが必ずしも明確に区別されていない。

②しかし BP については、優等生であってもすべてを守ることは現実的には難しい。

③ところが、ある組織全体の信用がたった一つの秘密漏洩ですべて崩壊してしまうことがある。上記で優等生的対応は難しいといったが、優等生的対応としての BP が期待されるところに、情報セキュリティのパラドクスがある。

④また秘密を守る技術も破る技術も日進月歩（分進秒歩？）で進んでいるため、今日の管理レベルが明日も通用するとの保証はない。管理義務のレベルも、これに伴って常時上昇していると考えざるを得ない。この意味でも BP 的対応は、時間とコストをかけなければ達成できない。

⑤現実に理想型を達成することができず、より低位の管理水準で秘密が漏洩してしまった場合の法的責任は、前述の義務違反型の場合と権利喪失型の場合とで、差をつけるしかないと思われる。同一のレベルで（たとえば「社会通念上認められた」という常套句が示すような世間一般の水準で）扱うことは、前者に重く後者に軽くなり過ぎるのではないか、と思われるからである。もっとも、このような一般化はそもそも不可能で、個別具体的事例に則して判断するしかないのかも知れないが。

⑥以上に伴う法的救済の可否は、すべて証拠いかんに左右される。情報という無形財に関する証拠能力と証拠（証明）力の問題は、有形の証拠の場合に比べて格段に難しい[72]。

８．情報セキュリティ法の体系化に向けて

以上に述べたところを暫定的に要約してみると、次のようになろう。

①現在の法体系は有形財を暗黙の前提にしたものであり、無形の財やサービス、とりわけ情報財を真正面から取り上げたものではない。

②したがって、秘密情報を一般法で規定した部分はごく限られており、実際に秘密を保護する必要性が高い場合には、特別法で対応してきている。

③しかし特別法は部分均衡を目指したものなので、これらの規定相互間に整合性があるとは限らない。特に違反行為に対する罰則にバラツキが見られ、その軽重を横断的に分析して合理性を付与する必要がある。

④また特別法の集合の欠点は、相互間に重複があったり、カバーできない領域が生じたり

[72] この問題も、注 10 に掲げた「電磁的記録の法的地位」で考察予定。

（法の欠欽）することである。この面からのチェックも望まれる。

⑤また仮に特別法が制定されたとしても、すべてを条文化することは難しいので、多くがガイドラインや規格に委ねられている。これらが法の目的に沿ったものであるか、権限を踰越したものでないか否かは、十分にチェックしなくてはならない[73]。

⑥②～⑤で述べたように、特別法には様々な問題があるが、秘密を一般法で保護すべきと考えた場合には、さらに根本的な問題が生ずる。すなわち、基本法的な性質で足りるのか具体的な義務規定を盛り込むのか、名宛人は誰か、いかなる秘密を対象にするのか、漏えいのみを禁じるのか無断利用を幅広く禁じるのか、行政法的に規制するのか民事法的または刑事法的に規制するのか、というように、多くの問題点に対する配慮が必要である。

⑦一方情報は拡散しやすい性質を持っているので、秘密を保護法益として法的に守る場合には、保有主体に対して拡散しないよう管理する義務が発生する。しかもそのレベルは、二重の意味で決定しにくい（相対的にならざるを得ない）。

⑧管理義務のレベルが相対化せざるを得ない第 1 の理由は、秘密を守ろうとする側と破ろうとする側の、力関係に依存していることである。これは日常生活において、たとえば三重に鍵をかけることが望ましい大都会の犯罪多発地帯と、昼間は鍵をかけなくても安全な農村地帯では、管理レベルが違わざるを得ないこととパラレルである（空間的相対化）。

⑨管理レベル相対化の第 2 の理由は、とくにデジタル時代においては、秘密を守る技術も破る技術も急速に進歩（進展？）するので、どの時点で見るかによってレベルが変化し得るからである（時間的相対化）。

⑩しかしこれらの困難を乗り越えて、「善管注意義務」や「自己の財産におけると同一の注意義務」とは別の、第 3 の注意義務レベルと設定しなければ、秘密保護の適正化を図ることはできない。

⑪その際には、法の一般原則に関する深い洞察と同時に、実務（企業における秘密の管理の運用実態）上の知識が不可欠である。この全く異なった 2 つの知識を融合することなしには、理論は空疎なものに終わるであろう。柿崎[2005]が試みたのは、監査論という企業統制の実践知と、法という理論との融合であった。情報セキュリティにつけても同様に、ISMS に代表される実践知と、秘密に関する法理論との交差・融合を試みることによって、新たな地平を開くことができそうである。

本稿のような初期的な考察においても、以上のような多くの示唆が得られたが、この経験を拡張して「情報セキュリティ法」を体系化することは可能だろうか。

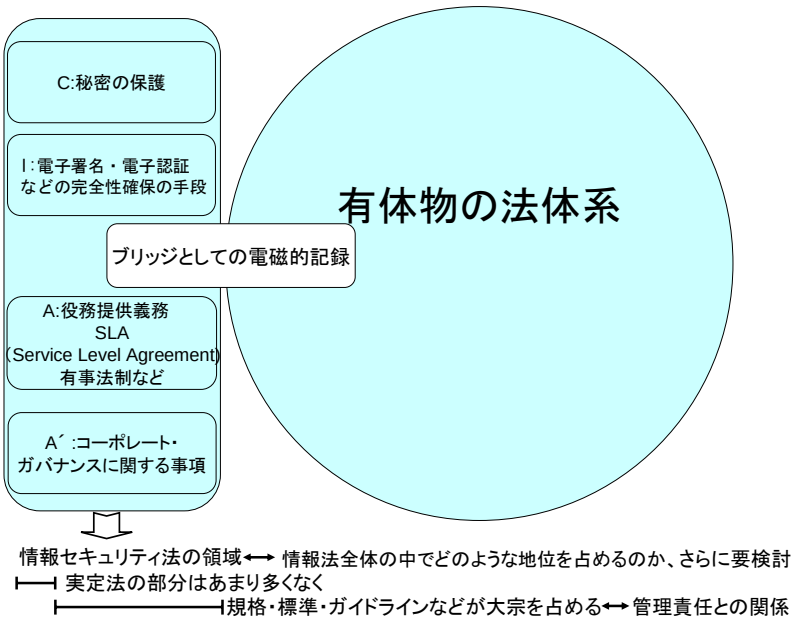
情報セキュリティの 3 大要素は、CIA すなわち Confidentiality（秘密性）、 Integrity（完全性）、 Availability（可用性）であると言われる。しかし最近はこれらが、Plan-Do-Check-Act のサイクルのうち前者に偏りがちであることから、Auditability（監

[73] このことは遵法精神に富み、コンプライアンスを「手順に忠実であること」と同一視がちなわが国では、とりわけ重要である。国際規約ではshallとshouldの区別があり、後者は通常「～が望ましい」と訳されるようだが、官庁の文書に「～が望ましい」とあると、受け取った業界はshallと同一視すると言われている。

査可能性） Acountability（説明責任）といった Check-Act の要素を加味すべきだとの主張もされている（前出の A と紛らわしいので、A´と表記しよう)。

これらの要素に対応するような法体系を構想するとすれば、次のようになろう（図表 12 参照)。

図表 12　情報セキュリティ法の体系化（試案）



（出所）筆者作成

①C に対応するものが、本稿で論じた「秘密」の法的保護に対応する部分である。

②I に関しては、電子認証・電子署名法ほか、いわゆる Forensics と呼ばれる手続法的な諸法が考えられる。本稿で触れながら別稿に譲ることにした「電磁的記録の法的位置づけ」は、I に関する法とも考えられるが、C や A(Availability)にも関係するので、図 4 では別建てにしておいた。今後の検討課題としたい。

③A(Availability)に関する法としては、通信・放送・電気・ガス・水道・鉄道・航空など、いわゆる公益事業における役務提供義務が該当するであろう。ハンディキャップのある人々に対するアクセシビリティの確保や、スパム・メールなどによって通信機能を麻痺させようとする企てに対する措置も含まれる。非常時に対応するものとしては、武力攻撃事態対処法や国民保護法などの有事法制も、この範疇に入るだろう。しかし、この分野は普通契約約款など契約法に依存する部分が多いと思われ、なお詳細な検討を要する。

④新たに追加すべき A´（Auditability and/or Accountability）に対応する法としては、いわゆるコーポレート・ガバナンスに関する諸規定が該当しよう。これを広く取れば、会社のあり方そのものを決めている商法のような基本法も入ってしまうが、ここでは企業の社会的責任(Corporate Social Responsibility=CSR)として論じられている項目に絞

っておく方が、合目的的であろう。

以上はあくまで試案の域を出るものではないが、幸か不幸か、このような体系化の試みは今のところなされていない。岡村[2003]、東倉ほか[2005]や松田[2005]など、こうした体系化の萌芽的試みはなされているが、いずれも実践知の面に偏りがちである。私自身の力量も限られているが、本稿における C に関する分析を踏み台にして、逐次各要素に関する研究を深めて、両 3 年内には「情報セキュリティ法」の体系的書物を書きたいと願っている。

[参考文献]

青山紘一 2005『不正競争防止法（第 2 版)』法学書院

Calabresi, Guido & A. Douglas Memaled 1972 “Property Rules, Liability Rules, and Inalienability: One View of the Cathedral” *Harvard Law Review* No.85

千葉大学 IP 研究会 2005「平成 15 年・16 年 不正競争防止法判決の統括（中)」、『特許ニュース』No.11481

茶園成樹 2004「営業秘密の民事上の保護」日本工業所有権学会 2004 所収

画像電子学会（編）2005『ディジタル情報流通システム』東京電機大学出版局

林紘一郎 1999a「ディジタル創作権の構想・序説―著作権をアンバンドルし限りなく債権化する」慶応義塾大学メディア・コミュニケーション研究所『メディア・コミュニケーション』Vol.49

林紘一郎 1999b「ⓓマークの提唱：著作権に代るディジタル創作権の構想」国際大学グローバル・コミュニケーション・センター『Glocom Review』

林紘一郎 2001「情報財の取引と権利保護」奥野正寛・池田信夫（編著)『情報化と経済システムの転換』東洋経済新報社

林紘一郎 2003「デジタル社会の法と経済」林敏彦(編)『情報経済システム』NTT 出版

林紘一郎 2004（編著)『著作権の法と経済学』勁草書房

林紘一郎 2005a「デジタルと著作権―法体系全体の再設計を」日本経済新聞経済教室欄、2005 年 2 月 15 日付

林紘一郎 2005b『情報メディア法』東京大学出版会

林紘一郎・石井夏生利 2005「秘密の法的保護―情報セキュリティ法を考える第一歩」『Cyber Security Management』2005 年 6 月～10 月号

林修三 1975『法令用語の常識（第 3 版)』日本評論社

堀部政男 1997「EU 個人情報保護指令と日本」ジュリスト増刊『変革期のメディア』有斐閣

堀部政男 2004「現行法ではヤフーBB 事件の再発は防げない一個人情報窃盗罪の新設を」文芸春秋『日本の論点 2005』

船越一幸 2001『情報とプライバシーの権利―サイバースペース時代の人格権』北樹出版

岩村智文 2001「盗聴法をめぐる法制審議会刑事法部会での審議」右崎・川崎・田島（編）
情報通信法制研究会（監修）2004『情報通信法令集』電気通信振興会
柿崎環 2005『内部統性の法的研究』日本評論社
経産省知的財産政策室 2003『逐条解説不正競争防止法』有斐閣
小塚壮一郎 2004「営業秘密をめぐる契約上の諸問題」日本工業所有権学会 2004 所収
Kohn, Linda T., Janet Colligan and Mollas S. Donaldson (eds.)2000 *To Err is Human : Building a safer Health System* National Academy of Science 医療ジャーナリスト協会(訳)2000『人は誰でも間違えるーより安全な医療システムを目指して』日本評論社
國井和郎・三井誠（編）2001『ベイシック法学用語辞典』有斐閣
牧野二郎 2001「インターネットと盗聴」右崎・川崎・田島（編）2001
升田純 2003「情報の売買」松本恒雄・升田純（編）『情報をめぐる法律・判例と実務』民事法研究会 pp.433-456
松田貴典 2005『ビジネス情報の法とセキュリティ』白桃書房
紋谷暢男 2003『無体財産権法概論』（第 9 版増補第 2 版）有斐閣
村上陽一郎 1998『安全学』青土社
永野秀雄 2004「サイバー戦・サイバー攻撃に対応するための国内法整備―特に機密情報保護のための人的セキュリティ制度の法整備について」『防衛法研究』No.28
中山信弘 1993『ソフトウェアの法的保護（新版)』有斐閣
中山信弘 1995「情報の流通と著作権」中山信弘・小島武司（編）『知的財産権の現代的課題』信山社、pp.210-224
日本工業所有権学会 2004『営業秘密の保護』有斐閣
西田典之 1998「個人信用情報保護と刑事罰」『ジュリスト』1144 号
小田中聡樹 2001「現代治安政策と盗聴法」右崎・川崎・田島（編）2001
岡村久道 2003「情報セキュリティ・マネジメントと法」㈶関西情報・産業活性化センター情報セキュリティマネジメント研究会『企業活動と情報セキュリティ』経済産業調査会奥平康弘 2001「いま市民的自由を語る意味」右崎・川崎・田島（編）2001
レッシグ、ローレンス・林紘一郎・椙山敬士・若槻絵美・上村圭介・土屋大洋 2005『クリエイティブ・コモンズ』NTT 出版
佐伯仁志 2002「刑法による情報の保護」宇賀克也・長谷部恭男（編著）『法システムⅢ情報法』放送大学教育振興会
佐久間修 1991『刑法における無形的財産の保護』成文堂
佐久間修 2004「営業秘密の刑事上の保護」日本工業所有権学会 2004 所収
苗村憲司 2005「営業秘密の秘密管理手段としての情報セキュリティ管理システムの役割」mimeo
青弓社編集部（編）2004『情報は誰のものか？』青弓社
園田寿 1999「刑法における情報の位置づけ」多賀谷一照・松本恒雄（編）『情報ネットワー

クの法律実務』第一法規出版
田村善之 1996「労働者の転職・引き抜きと企業の利益」『ジュリスト』1102～1103
田村善之 1999『競争法の思考形式』有斐閣
田村善之 2003『知的財産法（第 3 版)』有斐閣
東倉洋一・岡村久道・高村信・岡田仁志・曽根原登 2005『情報セキュリティと法制度』丸善
通産省知的財産政策室 1990『営業秘密』有斐閣
内田貴 2002「電子商取引(1)－サイバー空間の契約」宇賀克也・長谷部恭男（編著)『法システムⅢ 情報法』
右崎正博・川崎英明・田島泰彦（編）2001『盗聴法の総合的研究―「通信傍受法」と市民的自由』日本評論社
Warren, Samuel D. and Louis D. Brandeis1890 “The Right to Privacy” *Harvard Law Review* Vol.4, No.5
安富潔 2000『ハイテク犯罪と刑事手続』慶應義塾大学出版会
山名美加 2004「日本における秘密特許制度」日本工業所有権学会 2004 所収