「秘密の法的保護」のあり方から「情報法」を考える

林　紘一郎[1, 2]

概 要

「情報法」という表現は無定義のまま使われることが多く,その一般理論を考察する努力はないに等しい.本稿は,こうした流れに抗して「秘密という情報を法が保護するとはいかなることか」という設問を通じて,情報法のあり方を考えた結果の素描である.情報が溢れる現代社会においては「情報の自由な流通」が基本であり,法が関与するケースは限られている.私法における限定的な保護の方式は「知的財産型」と「秘密型」に分かれ,前者にはしかるべき注意が払われてきたが,後者は十分考察されてきたとは言えず,差止や刑事罰の可否の不統一にその欠陥が現れている.しかし特定秘密保護法と番号法の制定を機に,そうした不十分さは克服されざるを得ず,情報そのものに「対世的秘匿性」がある secret と,情報の授受当事者間の「関係性の中で秘匿性が判断される」confidential の二分法が,基本的視座になり得るであろう.本稿は,その二分法を検証することを通じて,知的財産と秘密を合わせた情報法の一般原理として,「差止条件付き許諾権としての知的財産制度」「管理責任付き秘匿権としての秘密保護法制」「情報と個人(または法人)の紐帯関係の基本としての帰属権」という,3 つの新たな仮説を提示している.

1　これまでの研究による知見と本稿の課題

「情報法」という表現は無定義で使われることが多く,その一般理論を考察する努力はないに等しい.唯一の例外に近いのは宇賀・長谷部(編)[2012] であろうが,これとても「情報法とは,情報の伝達,公開,保護等に関する法の総称」としているだけで,「情報」や「情報法」を幅広く捉えた上で,その「一般理論」を追求しようとする私の方法論とは距離がある[3].もっとも,かく言う私も「情報や情報法を細部まで定義してみよ」と逆襲されると,たじろいでしまう.このテーマについて書き始めると,何十冊もの本になってしまうであろう.それでは「乏しい知見でも分かち合って,難題に近づいていこう」という私の意図を伝える前に,私の生命が尽きてしまいそうである.

そこで,ここでは,「基礎情報学」の定式化を目指す西垣 [2004][2008] に依拠して,情報とは「生命体にとって意味作用を持つもの」で「機械情報・社会情報・生命情報」に区分す

---

1 情報セキュリティ大学院大学教授

2 本稿は,日本セキュリティ・マネジメント学会第 28 回全国大会(2014 年 6 月 21 日)における私の報告「Secret 対 Confidential: 秘密の法的保護の 2 態様」を,大幅に加筆・修正したものである.前稿と本稿の先行バージョンに対して的確なコメントをいただいた,名和小太郎・福家秀紀・山田肇・湯淺墾道の各氏に感謝する.コメントは十分咀嚼したつもりであるが,仮に誤りがあれば,一切の責任は筆者にある.

3 曽我部 [2014] には、こうした現状を克服しようという意欲が見られる.

ることができ「それによって生物がパターンを作り出すパターン」（西垣 [2004] p.27）であるとしておこう.ただし,世間一般がそうであるように,三種の情報のうち発展が著しいのは機械情報であるから,そこから始めて次第に生命情報に移行していくことをお許しいただきたい（西垣も,このルートで「情報学的転回」が起き得るとしている）[4].

本稿は,上記を仮の定義として,「秘密という情報を法が保護するとはいかなることか」という設問を通じて,情報法のあり方を考えた結果の素描とともに,検証すべき幾つかの仮説を提示するものである.情報が溢れる現代社会（情報社会）においては,情報の自由な流通（Free Flow of Information = FFI）が社会存立の基本条件の1つである.憲法が保障する「言論の自由」（内心の自由や表現・集会の自由なども含めた広義）は,この原理を直截に示している.もちろん,ここで「自由」というのは「無法」ではなく,「適法」という意味であり,「例外のない規則はない」の法格言のとおり,「言論の自由」が他の法益と衝突した場合の調整原理も検討しなければならない.

しかし総じていえば,公法の分野における「情報の法的位置づけ」は,かなり広範囲な検討と批判に晒されてきた.情報法を講じていると自称する人々の多くが,憲法や行政法などの公法学者であることは,この事実と符合している.これに対して私法分野のそれは,インターネットの発展に伴って法的な問題が急速に展開してきたこともあって個別的な対処に追われており,中でも注目されているのが個人情報や営業秘密の流出事件である.ここでは,前述の「情報の自由な流通」を原則としながらも,何らかの法的介入が無ければ社会正義が実現されないと考えられる場合には,それにふさわしい（過不足のない）法的救済手段を用意すべきという原則論では合意があるが,残念ながら具体策となると統一原理がないと言わざるを得ない.

しかも,そこには想像以上の難題が控えている.というのも,情報には有体物と違って ①「見たり触ったりすることができない」（intangible）もので,②複製が容易かつ安価で何度複製しても品質が劣化せず,③ 複製後も元の情報は残っている（非移転性・非占有性）ことに加え,④ 一旦引渡したら取り戻すことができない（取引の不可逆性）といった特性がある.したがって,「排他性・競合性」を前提にした「有体物の法体系」を,そのまま情報に適用することはできない（林 [1999] [2001] [2003a] ,池田・林 [2002]）からである[5].

わが国の法制度は,この事実を十分弁えていたと見え,私法の基本である民法は「この法律において『物』とは,有体物をいう.」と宣言して（民法 85 条）,無体財の扱いを知的財産法制などの個別法に委ねている.「法の謙抑性」がさらに要請される刑法においては,窃盗の対象に電気以外の無体財を含めない（いわゆる「情報窃盗」は罪にならない）ことを明らかにし（刑法 245 条の反対解釈[6]）,より慎重な扱いとなっている（林 [2011a] [2013a]）.

このことは,一般人の法への期待を損なってもいる.なぜなら「USB という有体物を盗めば窃盗だが,中身の情報を盗んでも罪にならない」という解釈は,一般の方には違和感を与え

---

4 このことは,法学にとって特段の意味がある.というのも,生命体（特に人間）の意思決定を最初に取り上げるとすれば,法律行為の基本としての「意思表示」（民法 92 条以下）をまず検討しなければならないが,それは相当の難題だからである.心理学や脳科学の成果と,この原理の整合性を分析するのは,容易なことではない.

5 もっとも「取引の不可逆性」が直接影響するのは,「変更困難な情報」（例えば DNA 情報）に限られ,ライフサイクルの短い情報（例えばクレジット・カード番号のように再発行＝変更可能なもの）は,さほどの影響を受けないとの見方もある.しかし,リベンジ・ポルノに見られるように,間に情報の仲介者がいる場合には,削除がままならない現状も忘れてはならない.

6 刑法第 36 章（窃盗及び強盗の罪）の保護対象は一義的には「財物」であるところ,刑法 245 条は「この章の罪については,電気は,財物とみなす.」と規定しているので,刑法の謙抑性からこれを反対解釈して,「情報は財物ではない」と解するのが一般的な理解である.

るからである.現に「人を欺けば詐欺罪になるが,コンピュータを欺いても罪にはならない」という不条理を解消するためもあって,「電磁的記録」という概念が導入されて,コンピュータ上の記録も有体物に準じた扱いをされるようになった(刑法 7 条の 2 など.林 [2005b]).こうした一見迂遠と思われる措置は,法の暴走を避け,その謙抑性を維持しているとも言える.前述のような特性を持つ情報に関して,情報窃盗罪を法定すれば,厳密な規定を設けたとしてもグレイ・ゾーンが残らざるを得ないため,公権力による拡大解釈の恐れが十分にあるからである.

いずれにせよ,この世の中に流通する情報量は爆発的に増大しつつあるが,その中で法的な保護の対象となる情報は限られていることを,まず確認しておこう(林 [2011b]).そしてこのことは,FFI を阻害しているのではなく,むしろ促進しているものと理解すべきである.わが国は「お上」に対する期待が必要以上に強いから,「適用法令がない」ことは国家のお墨付きがなく「不安が一杯」な無法状態であると理解しがちであるが,事実は全く逆で,「国家の介入がない」ことは「自由が拡大している」と考えるべきである(もちろんその場合には,自己責任の範囲が拡大せざるを得ないが).

2 情報の保護方式:知財型と秘密型

情報法がその対象である情報をどのように扱っているかを概念的に示したのが,図 1. である(初出は,林 [2011b])[7].

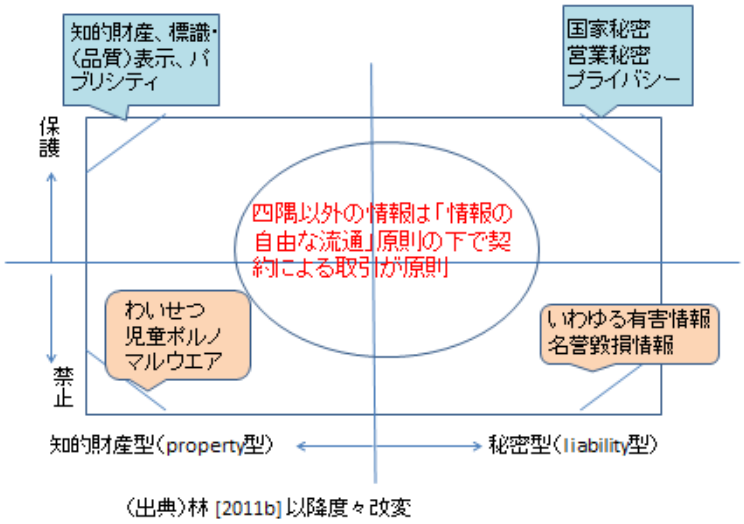

図1. 情報の保護と禁止の体系

この図において上半分は,法が情報を保護する場合の態様を示し,下半分は法がある情報類型について,その利用や流通を禁止する方式を示している.後者も「情報法」の対象であることは疑いないが,本稿ではまず保護の対象(つまり図の上半分)に絞って議論を展開

[7] ここでは,① 情報をとりあえず法の客体と認識し,② 当該情報はかなり狭い範囲で特定可能,という暗黙の前提を置いている.しかし ② については,いわゆるビッグ・データ時代には,全く違った角度からの分析を必要とするかもしれない(断片的な情報では特定されない個人が,ビッグ.データでは特定可能になるプロ・ファイリングの問題など)が,ここでは扱わない.

する[8].また図の左半分は,ある情報類型に対して法が予め権利を設定する方法(権利型,権利付与方式,property rule などと呼ばれる)を,右半分はある情報に関して何らかの関係性を有する者の利益が侵害された場合に事後的に救済する方式(利益型,事後救済方式,liability rule などと呼ばれる)を示している.なお図の一部は,林 [2013b] において補正されているが,その点については最後に触れる[9].

現行法における情報の保護方式は「知的財産型」(権利型)と「秘密型」(利益型)とに明確に分かれているが,読者に馴染みが深いのは,知的財産型の情報であろう.ビジネスマン(特にエンジニア)にとって特許は身近な例であり,誰でも創作者になれるデジタル時代には,著作権に関する知識が有益になる.加えて商標や意匠などの標識や,ブランド名などの著名表示に関するルール,さらにはパブリシティの権利などは,ビジネスの成否に大きな影響を与える.これらの情報は,いずれも公開(開示)されており[10],知的財産制度とは,「公開情報に権利を付与して保護する」仕組みである.

なお情報化社会の現代では,食品の消費期限・原産地などの表示や,個人の学歴や資格などを偽って表明すると,社会の指弾を浴びることが多くなった.また会社が公表する決算書類や監督官庁への報告に偽りがあると,相応のサンクション(金融商品取引法の罰則のほか,マス・メディアによる追及,認可や資格の停止等)を受けるなど,表示情報の大切さ(セキュリティ管理的な用語では integrity の意識)が高まっている.これらの情報は,現在は知的財産型に含まれていないものの,何らかの法的保護の対象と考えるべきだろう.しかし,そうした認識が行き過ぎ「これらの情報には,すべて誰かに権利がある」と考えると,誤解も生ずる.上記のうち,法が直接的・個別的に「権利」として保護しているのは知的財産法に属する情報だけで,多くは競業者間のルールである不正競争防止法や当事者間の契約や約款,それらを補う「信義誠実の原則」(民法 1 条 2 項)などの一般原理によって保護されているに過ぎない.

また法が保護してくれる「権利」も,有体物に関する所有権のような強い排他権が与えられるのではなく,前述した情報の「非占有性」「非排除性」「取引の不可逆性」等に配慮した「相対的に緩やかな排他権」が認められるにとどまっている(特許権における強制許諾,著作権における「公正使用」には,特許法 93 条,著作権法 30 条～49 条などの調整原理が働いている).つまり現行の法体系においては,物権と債権は明確に区別され,この中間形態を認めていないため,知的財産制度は所有権に近い構成(物権的構成)となっているが,本来なら「第 3 の権利類型」として扱われるべきものと思われる.その際の特徴を大胆に仮説化すれば,「差止条件付き許諾権」ということになろう.

もっとも,特許権と著作権の間にも,有意の差があると考えた方が当たっているだろう.というのも,特許権は ① 保護の対象が「請求の範囲」に限定され(特許法 36 条),② 出願―審査―登録という手続きが明確であり(同第 2 章,第 3 章,第 4 章), ③ 権利存続期間が出願後 20 年と相対的に短く(同 67 条),④ 出願後 18 か月で公開される(同 64 条)のに対

---

8 禁止の情報に関する分析を除外したのは,すべてをカバーする時間と能力に自信がないことに加え,禁止の分野が「言論の自由」との関連で,かなり分析されていることにもよる.情報法が時として「言論(の自由)法」と混同される傾向があるのは,この事実と関連があろう.ただし私は,「わいせつ情報」など「自由な流通」が認められない情報を「負の知的財産」と観念することで,私法の分野にも適用可能な統一原則を見出し得ると考えているが,今後の課題である.

9 また図の中央部分は「私的自治の原則」(契約自由の原則)に委ねられており,前節で述べたように,法的保護の領域が限定的であることも確認されたい.

10 審査中の特許情報は秘匿されねばならないが,出願後原則として 18 か月で公開される(特許法 64 条以下).ここに,「公開情報に権利を付与して保護する」という知的財産制度の特徴が,最も良く示されている.また,わが国には「秘密特許」(特許の存在そのものを秘匿することを許す特許)の制度もない.

して,著作権の場合は,(ⅰ) 創作性さえあれば保護され(著作権法 2 条一号),(ⅱ) 一切の手続きを必要とせず(同 17 条 2 項),(ⅲ) 存続期間が著者の死後 50 年(多くの国では 70 年)という長期で(同 51 条 2 項),(ⅳ) 非公開のものも保護される(同 18 条),という際立った差があるからである.

この両者の対比からすれば,情報の保護方式のモデルとしては,特許権の方が適していると思われるが,その適用対象となる情報の範囲は「発明」すなわち「自然法則を利用した技術的思想の創作のうち高度のもの」(特許法 2 条 1 項)ときわめて限定的である.そこで「情報法」の主たる役割が,ある種の情報の法的保護にあることを前提にすれば,(事実を示すに過ぎないデータなどを除いて)幅広く情報に権利を付与する著作権の方こそ,情報法のひな型にふさわしいと考えたいところである.

しかし,それが無理であることは上記の比較から明白であろう.アナロジーとして著作権を使うのであれば,(ⅰ) まずもって保護期間を特許権並みにし,(ⅱ) 何らかの形で登録したものをモデルとしなければ,バランスに欠けると言わざるを得まい(林 [2004],田中・林 [2008]).ここで「登録」とは,わが国の法律用語として使われている「権限ある公的機関が行なう登録」だけでなく,権限ある私人も登録できるものでなければなるまい.しかも,その方式は登録機関(registry)におけるものは当然として,それ以外のネット上の識別表示(クリエイティブ・コモンズによる cc. マークが代表例[11])をも許容することとすべきである(林 [2004],クリエイティブ・コモンズ・ジャパン [2005])

一方,もう 1 つの保護方式である秘密については,国民・企業(あるいは政府自身)が,「これが秘密です」と考えるものを,自分で秘匿する努力をしている限り,その流出等に対して政府が事後的な救済を与えてくれるものである.上述の知的財産のように,政府が「権利」に近い形で保護してくれる訳ではない.政府が保護の主体であるとすれば,その範囲を画定せざるを得ず,必然的に情報の仕分け=classification を行なわざるを得ない.政府がこれに関与すれば検閲に近いものとなり,FFI すなわち言論の自由が危うくなってしまうから,そのような仕組みは長所よりも欠点が多いと考えざるを得ないからである.裁判所は,秘密が侵害された後で被害者が損害賠償を求めた場合には,それに見合った補償をしてくれるに過ぎないし,差止は通常認められない(取引の不可逆性から差止の意味がない場合が多い).ごく一部について刑事罰が定められているが,その点については後述する.

したがって,知的財産と秘密は,民法の不法行為規定(709 条)における「権利または利益」にそれぞれ相当すると考えることもできるし,アメリカ法における property rule と liability rule(Calabresi and Melamed [1972])にも,ほぼ対応しているとも言える(林 [2010]).つまり,権利≒物権≒事前の権利付与方式≒ property rule に対して,利益≒債権≒事後の救済方式≒ liability rule という対照を推定することができる.もちろん外国法と比較する場合には,細部の微妙な差を無視することはできないが,「情報法の一般理論」という未だ解明されていない分野の仮説としては,検討に値するものと考える.

このような対照的な差を一覧表にしてみると,以下のようになろう.

11 Attribution(著者名を表示), No Commercial Use(非商用利用のみ可), No Derivatives(二次的著作物は不可,言い換えれば改変不可), Share-alike(改変可だが,改変前と同一の条件で他人の利用を妨げない)の 4 つの基本的権利表示を組み合わせて,合計 12 種の権利を表示できる仕組みとしてスタートしたが,後に Attribution を mandatory としたので,現在のオプションは 6 種類になっている..

表1．知的財産（権利）型と秘密（利益）型の対比

区分	知的財産（権利）型*	秘密（利益）型*
情報の保護方式	公開して守る	秘匿して守る
排他性と要式性	事前に禁止権（許諾権）を付与,著作権を除き方式主義	保護利益の侵害から事後的に救済.権利ではないので手続きは不要だが,事後的に裁判所から「利益」として認めてもらう必要がある.
法的効力	世間一般に対して（対世効）	関係当事者間において
排他性の限界あるいは自己責任	保護期間の有限性,強制許諾（特許権）・公正使用（著作権）など	法的な排他権がないので,情報の保有者に秘密を管理する責任が生ずる
救済,抑止手段	損害賠償,差止,刑事罰	損害賠償,（ごく一部について）刑事罰,差止は原則不可

* 権利と利益の区分は,民法 709 条における「権利」と「法律上保護される利益」に対応

表の左側すなわち知的財産型の情報には,従来からしかるべき注意が払われてきたが,もう1つの類型である秘密型のものについては,十分に考察されてきたとは言い難かった.それは,おそらく以下の諸要素が絡み合ったところから生じたものであろう.

① 最も秘匿性が期待される国家機密に関して,しかるべき法が存在しなかった.
② 企業の秘密としての営業秘密の保護について,秘密と考えるより知的財産と観念してきた.
③ 個人の秘密であるプライバシーに関しても,研究者の多くが憲法や行政法が専門であったためか,秘密の保護という認識が薄かった.
④ 実体法の議論が中心で,手続法的な救済の議論が乏しかった.

しかし,特定秘密保護法[12] と番号法[13] の制定を機に,そうした不十分さは克服されざるを得まい.なぜなら,そこでは以下のような新しい仕組みが導入されるからである.

① 特定秘密保護法において,秘密の指定と解除の手続きが明文化された（3 条と 4 条）,
② 同じく同法において,特定秘密を取り扱うことができる者に関する資格審査（security clearance）が明文化された（13 条～17 条）,
③ 一方番号法においては,個人番号という,それ自体は人格権的価値からは独立した情報に関して,これを秘密の一種とみなして刑事罰が法定化された（67 条～75 条.もっとも立法者には,秘密保護法の一種だとの認識は薄いようだが）.

3 Secret と Confidential：秘密の法的保護の2態様

それでは,秘密を法的に保護する場合の一般原則は何だろうか？ まず,一定の情報を秘匿したいとする場合に,法がそれを保護してくれるためには,3 つの前提条件が必要であることを確認しよう.それは当該情報の a）有用性, b）非公知性, c）秘密管理性である.なお a）については主観的なものではなく,客観性を要すること（客観秘あるいは実質秘）が,いわゆる西山事件に関する最高裁判決で確定している[14] .つまり「極秘」などのハンコが押されていれば自動的に保護されるのではなく,その内容が秘密として保護するに値するか

[12] 正式には「特定秘密の保護に関する法律」平成 25 年法律第 108 号. なお、その制定に先立つ検討として、情報保全システムに関する有識者会議［2011］参照）.
[13] 「行政手続における特定の個人を識別するための番号の利用等に関する法律」平成 25 年法律第 27 号
[14] 最一小決 1978 年 5 月 31 日刑集 32 巻 3 号 457 頁

どうかが問われるのである.

これらの要件は,営業秘密については明文化されており(不正競争防止法 2 条 6 項),地方裁判所のものながらプライバシーを最初に認めた判決においても前提とされていた(いわゆる「宴のあと」事件判決は[15],「私生活をみだりに公開されないという法的保障ないし権利」と定義している)が,秘密保護の一般原則であるとの議論はなかった.しかし,特定秘密保護法において秘密の指定と解除の手続きが詳細に定められたことによって,この 3 要件が他の秘密類型にも適用可能な一般原則であることが,明確になったものと思われる.

また,特定秘密保護法において営業秘密の管理方式(不正競争防止法 3 条 1 項の要件)が参照されていることからも,営業秘密は知的財産型ではなく秘密型の情報であることが,より鮮明になったと思われる.営業秘密が知的財産の一部と誤認されてきたのは,物権的な権利であるとの理解が一般的であったことに加え,差止請求権があることによるかもしれない(表1. を参照)が,それは誤解に近い.そうした事態が生じたのは,現行法においては差止めに関する一般的規定がなく,裁判官の裁量に任されていることにも一因があるのではなかろうか.

英米法において差止めは, common law ではなく equity に属するとされ,両裁判所が分離されていた時代にはエクイティ裁判所の専管に属するものとされてきた.そこでは裁判官の裁量が重視され,一般原則を定めるのは困難と理解されてきたが,今日のアメリカでは州際取引の予見可能性を高めるためもあって,Restatement で,要件が定められるようになっている[16].わが国では,不法行為による救済については,民法に一般原則が定められているが(民法 709 条など),もう 1 つの救済手段である差止めについても,民法に要件を定めるべき時がきたのではないかと考える(中村 [2014]).そこで,差止が認められるか否かという論点はとりあえず脇に置き,企業秘密を含めた秘密の法的性格をゼロ・ベースで考えれば,「管理義務付き秘匿権」という理解が最も適切であるように思われる[17].

ところで大方の読者は,国家の秘密である「特定秘密」と,企業の秘密である「営業秘密」が「秘密」のカテゴリーに属することには賛同しても,プライバシーが「個人の秘密」として秘密の一種に位置づけられることに,違和感を持たれるかもしれない.プライバシーは多義的な言葉で,特にアメリカにおいては「自己決定権」といった包括的な理念をも含むので,これを短い言葉で説明することはできない(林 [2011b] [2012] [2013b]).その法的根拠(特に憲法上の根拠)についても種々の学説があり,個人の人格と強く結びつけたものから,人格権とは切り離して alienable(取引可能)と考えるものまで,実に幅広い.また国際比較をしても,基本的人権の一種(それも最高位のもの)とする EU と,取引可能で property に近いと考えるアメリカ,プライバシー侵害訴訟を認めず breach of confidence を訴訟原因とするイギリスなど,先進国間でも理解が異なっている(林 [2012] [2013b]).

しかし,プライバシーから人格権的な要素をとりあえず捨象し,情報の一種という価値中立的な捉え方(冒頭に述べた西垣流の「機械情報」的扱い)をした場合,そこに前述の 3 要素,すなわち a) 有用性, b) 非公知性, c) 秘密管理性, を読み取るのは,さして難しいことではない.明文の規定はないが裁判において,ア) 主観的に過ぎる訴えは認められないこと,イ) 公知の事実は保護されないこと,ウ) 自ら明かした事実は保護されないことから,上記の a) ~

---

15 東京地判 1964 年 9 月 28 日下民集 15 巻 9 号 2317 頁

16 Restatement とは,判例を整理して一般原則を抽出し,州法の制定の際に参照してもらうことにより,合衆国全体の法の標準化を図ろうとするもの.差止については,Restatement (Second) of the Law, Torts(1979) の 934 条と 936 条が特に重要.

17 不正競争防止法における「技術的制限手段の回避」(2 条十号)や著作権法における「技術的保護手段の回避」(2 条二十号,30 条 1 項の除外規定二号など)と,「不正アクセス禁止法における「アクセス管理義務」が,管理義務付きという根拠を示している.

c) が含意されているものと見られ,プライバシーはやはり秘密の一種と考えるべきであろう.

ところで,秘密に対応する英語には secret と confidential の 2 つがあるが,後者の語源的な意味が,わが国では正しく理解されていないのではないかと思われる.というのも,この動詞型である confide とは「相手を信頼して情報を開示する」という意味であり,当該情報が秘匿すべきものか否かは,情報の授受当事者間の関係性に依存している.つまり,情報そのものが「如何なる状況でも秘匿すべきもの」という意味ではないからである(形容詞である confidential には,そのようなニュアンスが含まれているが.江口 [2010]).

ただし語源はともかく現代的な意味では,二つの語は別のものというより互換可能な概念として,理解されているようである.少し横道にそれる危険はあるが,言葉が意外に大切な意味を持つことがあるので,法律用語の辞典として名高い Black's Law Dictionary を引いてみよう.

Secret n. 1.Something that is kept from the knowledge of others or shared only with those concerned 2. Information that cannot be disclosed without a breach of trust; specif., information that is acquired in the attorney-client relationship and that either (1) the client has requested be kept private or (2) the attorney believes would be embarrassing or likely to be detrimental to the client if disclosed.

Confidential adj. 1. (Of information) meant to be kept secret <confidential settlement terms>

2. (Of relationship) characterized by trust and a willingness to confide in the other < a confidential relationship between attorney and client>

ここでは現代の用法に従って,secret と confidential は互換的な要素を持つものとして説明されているが,それでも secret の定義 1.と 2. との間には,有意の差があることが読み取れるであろう.しかも confidential の定義において,1.が「情報そのもの」に着目したものであり,2.が情報の授受当事者間の「関係」に着目したものであるとカッコ付きで補足説明されていることが注目される.もっとも,これは主として英米法における理解を前提にしており,(わが国を含む)大陸法系の国々においては,そもそも trust(信託)という概念が未発達であったため,両者を区別する意識がなかったように思われる[18].

ところで confidentiality という概念は,セキュリティの世界では「いわゆる CIA」の C として,一見すると最大限の尊重を得ているかのように見える.しかし他方で,国家機密などの情報の分類・格付においては,top secret > secret > confidential > non-classified という順序になり,confidential が必ずしも秘匿性が高いとは言えない.この順序は,秘匿の必要性の程度を表すと同時に,秘匿されるべき情報が,当該情報の帰属主体との紐帯を離れて(なお帰属という概念を法的にどう扱うべきかについては,後述する),世間一般に対する効果(対世効)を有する程度とも関連しているものと推定される.

そこで,情報そのものに「対世的秘匿性」があるものを secret と,情報の授受当事者間の「関係性の中で価値が判断されるもの」を confidential と理解することにより,秘密の保護法制のあり方を包括的に論ずることが可能かどうかを,検討してみたい.

4 秘密侵害に対する救済手段

しかし,その前に,秘密を法的に保護するといった場合に,どのような救済手段が前提にさ

[18] ドイツ語では secret が geheim に,confidential が vertraulich に当たるようだが,信託法の歴史がないためか,後者にぴったりの法律用語がないようであり,また独和辞典で「秘密」を引いても前者しか出てこない.

れてきたかを考察しなければならない.というのも前述のとおり,情報には「非排他性」「非排除性」「取引の不可逆性」といった特性がある以上,それらを克服することが技術的に可能であるかどうかが,法の実効性につながってくるからである.言い換えれば,秘密の一般原則に関する考察が乏しかった理由として挙げた4点のうち,④ の手続法の検討が先行すべきこととなる.

秘密が漏えいすることを防止し,万一漏えいした場合に受けられる法的救済は,第一義的には行為者に刑事罰を科すことだとされてきた(この考え方を仮に「刑事罰必須論」と呼んでおこう).しかし他方で(既に1. で述べたように)情報が持つ特質から,有体物を前提にした規定をそのまま情報財一般に拡大適用することはできないので,刑法で対象とされている「秘密に関する罪」は,信書開封罪と弁護士など一定の職業従事者の秘密漏示罪の 2 態様に限られている(刑法 133 条と 134 条).実は,この間隙を埋めているのが各種業法などの個別法であり,罰則を有するものを数え上げることはできないほどである.これらの規定を一般法である「刑法」に対して特別刑法と呼んでいる.その違反行為には一般の刑事罰が科されるが,そのうち行政命令に反する行為に関するものを,特に行政刑罰と呼ぶ[19] .

特別刑法において,秘密の保護レベルの均衡がとれているかどうかは,実は事後検証にさらされていないのではないかと疑われる.というのも筆者は,バランス論の一助として,特定秘密保護法の制定以前に,特別防衛秘密,防衛秘密,通信の秘密,国家公務員の守秘義務違反,のそれぞれの刑の長期を調べたことがある(林 [2005b])が,上記の順に 10 年＞5 年＞3 年＞1 年となり,バランスが取れているとは思えなかったからである.もちろん,刑の長期が唯一の指標ではないだろうし,新法の制定時には内閣法制局等を通じて,バランスの再調整が行なわれるであろう.ただ,時代の変化が激しい現代にあっては,保護すべき法益も急速に変化するものである以上,こうした見直しが適時に行なわれる必要があろう[20].

一方,民事的な救済を求めるのであれば,損害賠償と差止が考えられるが,情報が漏えいした場合の被害を事後的に損害賠償で償っても意味がないことが多い(第 1 節で述べた取引の不可逆性などのため).そこで,より多くを差止に期待せざるを得ないが,近代法において差止は 2 次的救済手段で,損害賠償をもってしては償えない損害であることを証明しなければならず,また裁判に要する時間を考えると,実効性に疑問が持たれているのが現状である.

そこで,片方で情報の社会的価値が高まり,他方でデジタル化によって漏えいや窃取が容易になる中で,刑事罰必須論に立つ個別法に実効性があるかと問われれば,甚だ心もとない.例を個人情報に取れば,その漏えいには刑事罰が直接科されることはなく,個人情報取扱事業者に不適切な運用があれば,主務大臣からの勧告・命令という手順を経て,最後の命令に違背した場合にのみ,法人に罰金が科されることになっている(個人情報保護法 34 条 2 項および 3 項と 56 条による間接罰.漏えい等の実行行為者に対する刑事罰がない点で,後述の番号法とは異なる).

世間では(特に個人情報取扱事業者を中心に)こうした現状に対して,直接罰がないことが抑止力の低下につながっているとする,刑事罰必須論が根強い.しかし漏えいが,報道されたものだけでも年間何百万人分にも及び,その暗数も無視できないほどと推定されるの

19 特別刑法はさらに,経済刑法と行政刑法の 2 種のタイプに分けられ,刑罰に至らない行政罰として過料がある.

20 法の拡大解釈などの懸念に対して,唯一安心材料があるとすれば,刑法の謙抑性の要請であろうか.刑事罰は個人の行為を前提にして科されるものであり,法人に直接科されるものとは理解されていない.そこで必然的に個人が持つ基本的人権との調和が要請され,謙抑的に立法され解釈されなければならないものと考えられてきた.

に,これに捜査当局がどう対応できるかは未知数である.

しかも刑事罰必須論は,厳罰化に傾くあまりか secret と confidential を混同する傾向がある.本稿で述べる立場からは,個人データは客観的で対世的効力のある secret となる場合は希で(後述の共通番号などは例外で),通常は confidential 型と考えるべきだろう.刑事法的には,仮に刑事罰を科すとしても親告罪が原則であることを,暗示しているように思われる.

そこで,刑事的救済に期待するよりも,民事的な「新差止制度」を工夫する価値があろう.その中心となる概念は現行のアメリカ方式とも言えるが,民事的な差止に加えて,差止命令を無視した場合に法定侮辱罪のような刑事罰を組み合わせることによって,より迅速かつ効果的な救済手段になり得るのではないかという点である.加えて,暫定的差止命令を迅速に処理できる体制を,整える必要がある(中村 [2014]).

なお,刑事罰を考える場合には,その構成要件が大切であり,秘密の場合には(積極的)知得,漏えい,窃用という 3 つの行為のうち,どの行為を違法とするか(全部か一部か)[21],どの程度の量刑が望ましいかなど多くの論点がある.また差止に実効性を持たせるため法廷侮辱罪のような刑事罰を加味した場合には,それが濫用されることのないような歯止めが必要である.現にイギリスのスーパー・インジャンクション(差止命令の存否も含めた守秘義務がある)が社会的な物議をかもしたような先例もある(Murray [2014] pp.139-149).

このように,さらに検討すべき論点は多いが,ここでは紙幅の関係から省略せざるを得ず,別途の機会を待つことにしたい.

5 秘密の分類と差止

それでは再び secret と confidential の二分法に帰って,これにより国家・法人・個人がそれぞれ有する「秘密」(すなわち国家秘密・営業秘密・プライバシー)はもとより,選挙における投票の秘密や「通信の秘密」,また入札情報やインサイダ情報さらには公益通報情報まで,どのように分類されるか,その分類と救済手段の間にはどのような関係があるかを検討してみよう.

上に掲げた各種の情報を 2 つの類型に分けると,以下のようになろう[22].

① secret 型:特定秘密,営業秘密,投票の秘密,入札情報,インサイダ情報,公益通報情報,通信の秘密のうち通信内容

② confidential 型:プライバシー関連情報,通信の秘密のうち制御情報

まず既述の類型以外のものについて,若干の補足説明をしておこう.

投票の秘密とは,公の選挙において「誰が投票したかしなかったか」や「誰に投票したか」といった情報が,秘匿されなければならないことを意味している.日本国憲法の第 15 条 4 項で「投票の秘密」が規定され,さらに公職選挙法 46 条 4 項で「無記名の投票」,同 52 条で「投票の秘密保持」が保障されている.投票の秘密が保障されない場合,投票先指図などの脅迫・強要,開票結果による報復,または買収・贈賄につながりかねず,正当な選挙が望め

---

21 通信の秘密に関しては,通信履歴(ログ)の保存は望ましいことなのか,逆に望ましくないのでできるだけ早期に削除すべきかが問題になっている.

22 もっともルールの常として,どちらに属するかを一義的に決めることができず,「時と場所と態様」(time-place-manner)という,環境の中でしか決定できない情報もあろう.この概念は,言論の自由を規制する場合には,「その内容には触れず(content-neutral),言論の取り扱い方で工夫することしか認めない」という視点から生まれた知恵である.例えば「誰かが不治の病である」という情報は,通常は秘匿すべきプライバシーに属するが,その主体が政治家や会社の社長である場合には,開示が強制される場合があると考えられる.

なくなり,延いては民主主義の基盤が危うくなるからである.

入札情報とは,物品やサービスの購入において相対(1 対 1)の取引をせず,入札情報を公告して参加申込を募り,希望者同士で競争に付して契約者を決める方式である.日本の官庁発注案件においては,一般競争入札とすることが,会計法第 29 条の 3 に規定されている.この場合の入札情報は,落札者が決定するまで秘匿しなければならない.落札後も落札者に関する情報は公開されるが,それ以外の情報は引き続き秘匿され,一定の期間を経過すれば消去される.

インサイダ情報とは,株式等の金融商品の取引に役立つ情報のうち,会社の業績の変動,画期的な新製品等に関する重要な情報等で,投資家に公表される前のものを言う.こうした情報は,a) 有用性, b) 非公知性, c) 秘密管理性が顕著であるため,明らかに法的な意味での秘密の要件を備えている.しかも金融市場における取引は,参加者間に構造的な「情報の非対称性」がないことを担保した上でなされるべきなので,インサイダ情報の漏えいや窃用は厳しく処罰される.

公益通報制度は,国民生活の安心や安全を脅かすことになる事業者の法令違反の発生と被害の防止を図る観点から,公益のために事業者の法令違反行為を通報した事業者内部の労働者に対する,解雇等の不利益な取扱いを禁止するものである.会社の法律違反行為には,「国民の生命,身体,財産等の保護にかかわる法律」として定められた 413 の法律が含まれる.この制度に基づいて通報された情報も,a) 有用性, b) 非公知性, c) 秘密管理性を満たすもの,つまり法的な保護の対象となる秘密として扱わねばならない.

これらの秘密に対して,通信の秘密は若干特異な扱いをされてきた.というのも,わが国の憲法には「通信の秘密を侵してはならない」という規定があり(憲法 21 条 2 項後段),かつては通信の事業主体が独占の公的機関(電電公社や旧 KDD)であったこともあって,国家権力による検閲が禁じられるべきという立場(憲法 21 条 2 項前段)と,同質のものとして論じられてきた歴史がある(林・田川 [2012]. 中世以降の郵便の歴史が,その実検閲の歴史であったこととも関連がありそうである).しかし現在の電気通信は,① インターネットが中心であり,② サービスも電話以外に多様化し,③ 事業者も多数存在し,④中央統制的な機関は存在せず,⑤ 「コモン・キャリアは通信内容にタッチすべからず」といった旧式の規制が意味をなさなくなっている(インターネットと通信の秘密研究会 [2013],田川 [2013]).

そこで新たな分析枠組みが必要になるが,その要諦は,通信内容と付帯的情報を分けて考えることであろう.通信内容そのものは secret であり,通信内容そのものではないが通信を接続するための付帯的メタ情報(あるいは制御情報.例としては,発信 ID,着信 ID,通信時間,プロトコルなどや,それらを記録したログ情報)は confidential 型と分けて考えれば,この二分法が充分役に立ちそうである(林・田川 [2012]).というのも,前者は対世的効力を有する秘密として厳格な適用を確保しつつ,後者については「顧客が事業者に期待する秘密」として,やや弾力的な解釈の余地を残すことが,サイバー犯罪の捜査などで期待されているからである(林[2013d])[23].

---

23 この部分の指摘は,個人情報とプライバシー関連情報の整理に関して,特別の意味を持つのではないかと思われる. というのも、繰り返し述べてきたように「情報は占有という独占的保有に馴染まない」から,1 対 1 の信頼関係を前提にして渡された(confide された)としても,いずれ第三者の手に渡ることは必至である. とすると,1 対 1 の段階の関係は confidential 概念で整理できたとしても,その情報が第三者の手に渡った段階以降の措置は,secret 的な扱いを組み込まないと,十分ではない恐れがあるからである.個人情報とプライバシーに関して議論が錯綜しているのは,このような視点を持って初めて理解できるのではないだろうか(林 [2011b] [2012] [2013b]).

以上で述べてきたことを総合して,この二分法とすでに提案した「新差止制度」との関係を図解すれば,以下のようになろう.ここで,有体物の法体系を参照しながら,新しい制度の持つ意義を述べよう.

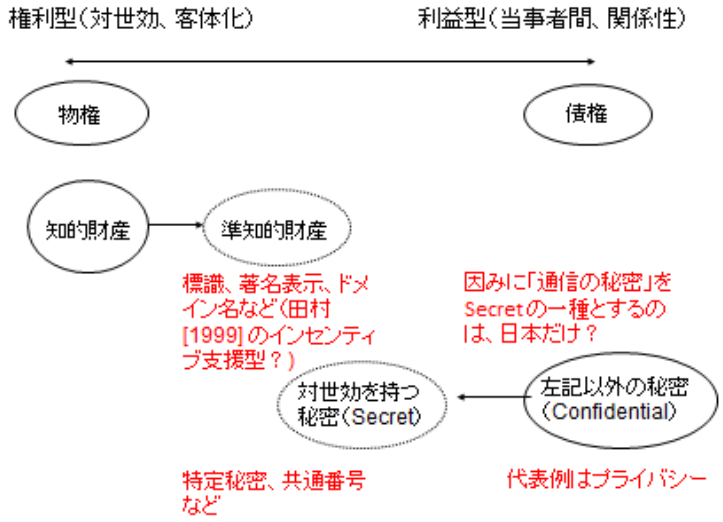

図 2. 情報財の法的保護態様

まず,有体物の保護方式は,物権型と債権型に明確に分けられている[24].前者は法律で決められたものしか認められず（物権法定主義,民法 175 条）,不動産では登記があれば（同 177 条）,動産では引き渡しがあれば（同 178 条）,第三者にも対抗できるよう定められている.これらが既述の対世効である.一方債権は,法に定められた定型的なもの（典型契約）のほか,契約によって自由に生み出すことができるが（契約自由の原則）,物権のような世間一般に対する効力を期待することはできず,原則として当事者間で（場合によっては,悪意の第三者まで含めて）効果があるだけである.

このように物権は,他人の利用を排除できる権利（自ら使用するだけでなく,賃貸・譲渡・利用許諾・担保権の設定などが自由に行なえる）と考えられているから[25],他人が権利を侵害しているときには,これを排除できるものと考えられ（妨害排除などの物権的請求権）,差止請求権も,その「権利の束」の中に入るものと考えられてきた.そのためもあって,従来の差止は（既に述べた点も含めて）以下のような欠点を内包しており,「意に反する情報漏えいの差止」を考える上では,ネックになっていたと言わざるを得ない.

① 発生史的な経緯（特に英米法においては,損害賠償と差止は別の裁判体系に属していた）もあって,損害賠償が第一義で,差止はそれを補うものと考えられてきた.
② 有体物に関するものを念頭に置き,原状回復を目指していた.その後人格権侵害や公害訴訟には拡張されてきたが,情報流通を対象にする考察は乏しかった.
③ 原則が法定されず,裁判官の裁量に委ねられてきた.これは上記 ① に沿うもので,柔軟な運用を目指したものだが,制定法主義が徹底しているわが国では,適用が限定される結果をもたらしていた.

---

24 これは,いわゆる大陸法系の国々では顕著であるが,英米法系の国々においても前述の property rule 対 liability rule として,主として救済手段の面から支持されてきた見方とも言える.

25 物権の代表格である所有権について,民法は「所有者は,法令に制限内において,自由にその所有物を使用,収益,処分する権利を有する.」（206 条）と規定する.

以上は有体物を中心とする法の考え方の説明であったが,情報についても同じように考えるのが常識化していた.つまり,法的な権利が明記されたもの（知的財産が代表例）には対世効があるので差止がデフォルト的に認められるが,それ以外の情報については,例外的な事例を除いて認められない,とするのがこれまでの通説であった.しかし,インターネットを介した情報の流通が一般化し,日々膨大な情報が世界を駆け巡る現代にあっては,このように差止を「継子扱い」することから脱却して,そのあり方を抜本的に見直すでき時期が来たと考えるべきだろう.

その際には,次の検討が必要かと思われる.

a) 民法には損害賠償の規定はあるが（709 条以下）,差止の規定はないので,これを明記する.
b) 恒久的差止と一時的差止の両方を規定し,それらが認められるための要件を明示する.

なお差止は救済手続の一種なので,民法ではなく民事訴訟法等の手続法で規定すべきだという意見があり得るが,インターネットの世界では「手続きがすべて」（Lessig [2000] の表現では,Code is Law.）の側面があるので,損害賠償と同じ法律に規定するのが望ましいと考える.しかし,一般条項をすぐに定めることにはリスクも伴うので,「小さく始めて大きく育てる」という慎重な対応が望ましいだろう[26].

そのような反省の上に立てば,図1. は余りにも割り切りすぎではないか,との批判があり得るであろう.差止の拡大の必要性について述べたことからも分かる通り,今後の方向性としては,両者の相互浸透を一定の条件の下で認めることが必要かと考える（図 2.）.つまり,権利（知的財産）型の中に,本来の知的財産が入ることは間違いないが,それに準ずるもの（先に述べた標識や表示情報,パブリシティなどの準知的財産）を加えるとともに,利益（秘密）型に属するものの中にも,特定秘密や番号法における番号など secret として対世的効力を認められたもの（対世的秘密）を認めることが必要だと思われる.

これは一見すると,これまでの私の研究を否定する要素を持っているかに見えるが,実は私は一貫性が失われるとは思っていない.「例外のない規則はない」という法諺があるように,原則と例外の関係が明確であれば,一定の条件を満たす例外が登場するのは,理論の破綻を意味するのではなく,むしろその頑健さ（robustness）を補強すると考えているからである.

6 秘匿と公開

ところで,秘密に関して世間一般にある誤解は,一旦秘密と指定されたら,その情報は永久に秘密扱いされるもの,という見方である.実態は全く逆で,秘匿には必ず「期限」があるから,いずれは公開されざるを得ない.つまり原則と例外が逆で,「情報はすべて公開の運命にあり,保有する主体が努力すれば一定の期間に限り秘匿することができる」と考えるべきだろう.先に挙げた,秘密を保護する前提としての 3 条件の中に,秘密管理性が入っているのは,このような意味に解するべきである.秘密として例示したものの中でも,入札情報やインサイダ情報には,このような「秘密の有限性」という特徴が良く現れている.

これを言い換えれば,図1. で示した「全体の中で法的な保護の対象になる情報は限られている」という理解が,秘密を扱う場合の原点でもあることを意味している.また政府機関

[26] 著作権法における一般条項としての「公正使用」（日本版 fair use）でさえ頓挫したのだから,最初は個人データ漏えい事件など特定の類型に対して差止が有効か否かを試すなどの「試行」が必要であろう.特別法を作って有効性を確認した上で一般法化するのが,賢いやり方かと思われる.

が保有する情報に関して言えば,およそ税金で取得・加工・保存された情報は原則として国民のものであり,秘密として管理される期間を過ぎれば,国民には「知る権利」があると考えるのが妥当である.現に,最も厳格な秘密管理システムを定める特定秘密保護法においても,以下のような規定が置かれていて,秘密の指定が時限的なものであることを明示している[27].

① 指定期間は,原則として 5 年である(同法 4 条 1 項).
② 延長は可能であるが,5 年ごとに延長措置を講じなければならない(4 条 2 項).
③ 通算して 30 年を超えて秘密を保持したい場合には,行政機関の長は「政府の説明責任の観点に立ってもなおやむを得ないものである」ことについて,内閣の承認を必要とする(4 条 3 項,4 項柱書).
④ 60 年を超えて秘密を保持できるのは,法に規定された 7 項目に該当する情報に限られる(4 条 4 項但し書き)
⑤ ③で内閣の承認が得られなかったものは,国立公文書館に移管される(4 条 6 項).
⑥ 指定期間の途中であっても,指定の条件を満たさなくなった情報は,直ちに指定解除される(4 条 7 項).

以上のように,特定秘密であるためには各種の条件と手続きを満たす必要があり,行政機関の長といえども恣意的に指定できないようになっている.もっとも,この点についての懸念が払拭された訳ではない.というのも,縦割りの官庁組織においては,「わが省にとって秘密である」ことが第一優先とされ,国家全体として見れば公開が望ましい情報が,必要以上に秘匿される危険があるからである.その意味では,指定権者(行政機関の長)からは独立した第三者機関による監視が不可欠であるが,この面でもわが国の仕組みと伝統は頼りない.特定秘密保護法においては,独立した諮問会議が法定されている(18 条)ほか,年 1 回国会への報告が義務付けられている(19 条).しかし実際の運用の細部は,政府が定める統一的運用基準に委ねられており,また内閣総理大臣の裁量の範囲が広い(穴戸[2013]).

このうち国会の監視については,衆参両院とも「情報監視委員会」を設置する法律が成立し,特定秘密保護法の施行(2014 年 12 月予定)と同時に発足する予定である.しかし既に,委員会の要請があった場合しか開催されず,各省庁が秘密の提供を拒んでも意見を表明することしかできないことが,批判されている[28].これは,先進諸国のレベルに比べても,著しく省庁優位になっているが,事は議会(立法府)対官庁(行政府)のバランス論や,法律の建付けばかりではないように思われる.

なぜなら,小は論文査読における著者と査読者間の応答(直近では小保方晴子氏対理化学研究所という図式も同じである)から,大はコーポレート・ガバナンスにおけるモニタリングのあり方(世界に希な制度である監査役の活かし方)に至るまで,わが国では「相互評価」や「第三者チェック」が根付いていない感があるからである.その結果,適正なチェックはなかなか実現されず,大部分は形式的なものに終わり,ごく希にチェックが行き過ぎると相互不信に陥る,といった結果に終わることが多い.これは一面では,民族的にも言語的にも多様性が乏しいわが国が持つ,宿命とも言える欠陥である.しかし,経済的にも政治的にもグローバル化が避けられない趨勢である以上,グローバル・スタンダードを墨守する必要はないが,これに comply することを意識しておく必要があろう.現に企業活動のグローバル化に伴って,独立取締役(社外取締役)の法定化や,コーポレート・ガバナンス・コードの制定と遵守(コ

27 なお本来なら,特定秘密保護法の全容を説明した上で個別の論点を紹介すべきであるが,政省令はなお準備中であるため,直ちに個別論に入ることをお許しいただきたい.全体像については,さし向き内閣官房「特定秘密保護法関連」サイト[2014] を参照されたい.

28 2014 年 6 月 20 日付毎日新聞など.

ードに反する場合には説明責任が生ずるとする comply or explain の原則）などが浸透しつつある[29].

なお,ここでも comply という語の理解そのものが,わが国では誤解されがちなことに触れておかねばならない.わが国でコンプライアンスは「法令順守」と訳され,「ある規範や基準があって,自分の行動等をそれに合わせる」ことと理解されることが多い.その結果,規範の内容よりも形式が優先され,さらに行き過ぎが起きると当初の規範の目的は忘れ去られ,「規定に合っていさえすればよい」,挙句の果ては「書いてないことは勝手にやってよい」という弊に陥ることさえある.

ところが,英語の comply を辞書で引いてみると,最後の方に「（機械の分野では）順応する,伸縮する,柔軟である」といった訳が出てくることに驚かされる.しかし機械工学の出身で「失敗学」の提唱者である畑村洋太郎教授に直接伺ったところ,バネが伸び縮みして弾力性を確保することが,comply の原点であるという.とすれば,わが国の理解は,著しく偏ったものと言わざるを得ない.

このような風土の中で特定秘密の指定が行なわれると,指定の要件を厳密に守るという利点が生まれる反面,「一旦指定されたら,なかなか指定解除しない」という弊害が主ずるであろうことは目に見えている.その結果は,特定秘密がどんどん集積され,解除する勇気がないままに年月が過ぎ,漏えいのリスクが幾何級数的に伸びていく姿である.

7 公開を前提にした保護のあり方

このような悪循環に陥るのを避ける方法はあるのだろうか？ その第一歩は，a） 情報は自由な流通が基本であること，b） 法が関与するのは自由な流通が社会的に深刻な被害をもたらすことが明らかである場合か，c） 自由な流通が阻害された場合に，その阻害要因を除去する場合に限られることを，理解し得心することではないかと思われる．その意味では，政府情報に限定されたものとはいえ，情報公開法の理解が基本になろう．

そしてその原型として，アメリカ合衆国の「情報自由法」（Freedom of Information Act of 1967，略称 FOIA）が参考になる．この法律は，民主主義の維持・発展のためには国民に広く情報が行き渡ることが不可欠であり，政府が保有する情報はなるべく早期に国民に還元すべきである，という強い信念に基づいて成立したものだからである．後者について，政府情報がふんだんに，かつほとんど無料で手に入るアメリカと，白書でさえ著作権があるとするわが国（著作権法 13 条二号の反対解釈）を比較してみれば，その差は明らかであろう．

もちろん，この法律にも欠点はある．とりわけ，情報公開請求の処理に膨大な時間とコストがかかっていることは，広く批判の的となってきた．わが国の場合も，官僚の側からは「一部のマニアックな開示請求者のために税金を使うのは無駄」という批判がよく聞かれる．しかし，民主主義にはそれ見合いの費用がかかるものであり，憲法補正 1 条において「言論の自由」を保障し，裁判においても他の法益に優先する評価を与えてきたアメリカが，情報社会で優位に立っていることは，決して偶然ではなかろう．

その証拠となる事実を 2 つ上げておこう．

第 1 は，外務省公電漏えい事件（前述のいわゆる西山事件と同じ．注 13 参照）と，それに類似するペンタゴン文書事件の対比である．前者においては，外務公務員と情を通じて秘密文書を入手した行為が可罰性ありとされたが，後者においてはベトナム戦争の経緯に関

[29] http://bdti.or.jp/node/1003 などを参照.

する秘密文書(″History of U.S. Decision-Making Process on Viet Nam Policy, 1945-1968″)をニューヨーク・タイムズに渡したエルスバークは,事実を明らかにすることが言論の自由に合致するとして,無罪となっている[30].

第 2 の例は,アメリカの情報自由法がイギリスのそれに与えた影響である.同じ英米法に属しながら,イギリスでは公務員の秘匿特権が強く「情報自由法」が制定されたのは 2000 年になってからである.その契機の 1 つに,英米両国の外交関係の文書がアメリカでより早く入手可能で,イギリスが秘匿し続けることが自国民に不利益を与えるとの認識があったといわれる(田中[2003]).

もちろん他方で,アメリカは安全保障に敏感な国でもある.今回,わが国の特定秘密保護法で保護される対象情報は,アメリカでは当然非開示に該当するものばかりである(永野[2013]).しかし同時にアメリカでは,政府情報を秘密指定期限が切れる前に公開したり,研究者にも security clearance を行なって情報の利用を許すなど,情報を利用した安全保障にも十分配慮している(土屋 [2007]).特に,建国当初から歴史的文書を組織的に保存すること(archive)に熱心で,国立公文書館を中心に「こんなものまで」と思えるほど資料を収集し,できるだけ公開している.特に大統領に関する情報は豊富で,プライバシーよりも公共の利益を優先させる姿勢が顕著である(ウオーターゲート事件や,クリントン・スキャンダルなどを想起せよ).

一方わが国には,情報公開法ができたのが 1999 年,公文書管理法が 2009 年という浅い歴史しかない.国立公文書館法は,情報公開法と同時期の制定で,それ以前に公文書館法が 1987 年に制定されているが,両法の成立以後においても,外務省外交史料館・宮内庁書陵部・防衛省防衛研究所図書館等が所蔵する図書等は,情報公開法の対象文書から除外されている(宇賀 [2010]).

このように公的資料を公開することは,外国政府等を利するばかりで,自国(民)が得るものは少ないと考えるかもしれない.しかし情報社会にあっては,公開情報を徹底的に考察して基礎を固め,なお必要な微妙なインテリジェンス情報に限って,シグナル・インテリジェンス(シギント)やヒューマン・インテリジェンス(ヒューミント)に期待することで,比較優位が確保されることは常識化しつつある[31].そして,国民の多くがインテリジェンス活動を不可欠の活動として認めている.現にスノーデン事件という,国家安全保障政策を根本から揺らがす大事件の後でも,情報収集の行き過ぎについての懸念はあるものの,アメリカの世論が NSA(National Security Agency)などを直ちに廃止せよという方向に動くことはないのである.

このような事実を踏まえれば,ごく狭い範囲の情報を,ごく短期間に限って秘匿し,秘匿の利益に見合ったコストで管理できなくなればいち早く公開するというメリ・ハリの効いたシステムを構築することが,今後の基本政策になるであろう.この意味でも,アメリカの経験に学ぶべき点は,多々あるものと思われる(永野 [2012]).

8 情報法への一般化仮説

これまでの分析から私は,以下の仮説を立てた.

［仮説1］ 現行の法体系においては,物権と債権は明確に区別され,この中間形態を認めていないため,知的財産制度は所有権に近い構成(物権的構成)となってい

30 New York Times Co. v. United States, 403 U.S. 713 (1971)

31 一説によれば,現在ではインテリジェンスの 7～8 割が Open Source Intelligence だと言われる.

るが,本来なら「第 3 の権利類型」として扱われるべきものと思われる.その際の特徴を大胆に仮説化すれば,「差止条件付き許諾権」としての知的財産制度ということになろう[32].

［仮説 2］他方, 秘密の法的保護について一般論を展開した論文は少ないが, その特質は上記の裏命題となり「管理義務付き秘匿権」ということになろう. 営業秘密について差止めが法定化されているため誤解されやすいが, 差止が認められるか否かという論点はとりあえず脇に置き,企業秘密を含めた秘密の法的性格をゼロ・ベースで考えれば,上記の理解が最も適切であるように思われる.

なお上記 2 つの仮説については,お断りとお詫びをしなければならない点がある.それは,林［2009］における説明とは,著しく異なる点があるからである.林［2009］を執筆した当時の私は,「個人データ」が知的財産的な扱いにふさわしいのか,それとも秘密的に扱うのが良いのかについて自信がなかった.と言うより,その両者の間に,本稿で説明してきたような著しい差があるという認識すら欠いていた.そこで,個人データの扱いを著作物とのアナロジーで論じたため,後述の「帰属権」についてはさほどの差がないが,「差止条件付き許諾権」と「管理義務付き秘匿権」を同列に並べて,「ライセンス利用権」と「保用権と義務」を含む「関与権」という 1 つの権利と考えるという,何とも初歩的な説明をしたに過ぎなかった.この点は本稿で抜本的に見直したので,その旨お許しを乞いたい.

今後は,これらの仮説を検証していく番だが,実はそこには私自身も意識していなかった,より重要な知見が隠されているように思われる.それは,法学の一般的方法論である「主体」と「客体」という分類が,情報法にもそのまま適用可能かどうか,という大問題である.プライバシーの分野で,「情報主体」という言葉が使われるときには,主体は人間であり客体である情報に,何らかの支配権（その最も強力な主張は「自己情報コントロール権」）を及ぼし得る,ということを暗黙の前提にしている[33].

しかし,有体物のように完全な排他権を観念できるものとは違って,情報には完全な「排除可能性」（他人の利用を排除することが技術的にも経済的にも可能である性質）も,完全な「競合性」（ある人が使っていれば,他の人は使うことができないという性質）もないからである（林［2009］）.説明を変えれば,「情報は誰のものか」と問われれば,「私に属していると思われる部分はあるが,全部が私のものとは言えない」というケースが殆ど,ということである（この点を含めて「情報は誰のものか」に関する良書は,同じタイトルの青弓社編集部［2004］である）.

とすると,「主体」である私が,「客体」である「私に関する情報」を支配する,という見方は偏っていることになる.支配できる程度がゼロではないが,100%もあり得ないからである.この点で,再び著作権法の助けを借りれば,「氏名表示権」という概念は暗示的である.日本語では語感が伝わりにくいが,英語の表現である ‘the Right of Attribution” は本質を突いている.Attribution とは,「ある事柄を,誰かに帰すことができること」を示しているからである.

つまり,ある著作物がある著者の創作にかかることを示すが,それ以上でも以下でもないことを意味している.この用法を拡張して,例えば私のことを記述した「個人データ」があって,その情報が「私に何らかの関係がある」と考えることができれば、それが attribution である（良い訳かどうか自信がないが,とりあえず「帰属」としておく）.その場合,私には当該情報

32 この定義自体,今後の批判に耐えなければならない「仮説」に過ぎないが,知的財産基本法における定義（同法 2 条 1 項）に比べれば「より理論的」であり,また「営業秘密」を知的財産として扱わず「秘密」の一種とするなど,新規性と進歩性を持つ主張だとするのは,いささか僭越であろうか？

33 プライバシーを専門にする学者の間では,情報に関するプライバシー権として「自己情報コントロール権」を前提に議論する向きが多いが,情報に（有体物に対するような）「排他権」を設定することはできないどころか,有害でもあることは,本稿を読まれた読者には説明を要しないだろう.

に関する何らかの権利が発生する,と考えるのが理に適っている.しかし,それは有体物に関する所有権のような「排他権」ではあり得ない.

このような権利を「帰属権」として定めることによって,上記の ① や ② の理解がスムーズになるものと思われるので,ここでは情報法の第 3 原理として,以下を追加しよう.

［仮説3］ ある情報が,ある特定個人（や特定法人）と関係が深いと思われる場合,当該個人（または法人）には,当該情報に関する「情報と個人（または法人）の紐帯関係の基本としての帰属権」が生ずる.

いずれにせよ,情報法に関する理解を深めれば深めるほど,そもそも「人間が主体で情報は客体である」というこれまでの法常識をも,覆す可能性を示してもいるように思われてならないが,これは意外な発見であった.

9 今後の課題

結びに当たって,ここまでの記述とは一見矛盾するような指摘を 3 点ほどして,今後の課題としよう.

まず第1点として,そもそも秘密を守ることは正しいことなのか,という根本的な疑問がある.両親が幼い子供に教える躾の中には「嘘をついてはいけない」とともに「隠し事をしてはいけない」が入っていることが多い.だとすれば,法律が秘密を守る必要はなく,むしろ公開を迫るべきではないのか？

「法と経済学」の創始者の1人で,意表を突く指摘で有名なポズナーは,「原則的には秘密は悪いことだが,なぜか例外的に認められるケースがある」として,人前では裸を見せないこと,恋人に良く思われたいためにある程度の隠し事をすること,などが許されるとしている（ベッカー・ポズナー［2006］）.第7節で述べた私の見解（公開が原則で,時限的に秘匿が許される）も,これに似た発想だと思っているが,それで十分なのかどうか,なお検討を続けたい.

第 2 点は,情報の保護方式として,まずは知的財産型と秘密型を峻別する立場をとったが,私自身がすでに峻別説の弱点を見つけている（林 [2013b]）.その要点は,秘密型は知的財産型と同様に,自然人が情報の主体で情報（秘密）はその客体という理解を前提にしているが,主客が完全に分離するのではなく,両者の関係の中で処理すべきことがあるのではないか,という視点であった.このような理解に至ったのは,同じ英米法に属しながらイギリスにおいては,プライバシー侵害に関して独立の訴因として認めず,情報の授受者相互間の confidence 違反（breach of confidence）して処理していることを知ったからであった（Richards and Solove [2007]）.

ここでも,先に述べた confide という動詞の意味が問われていることが注目されるが,より重要なのは,アメリカではプライバシーは確立した「権利」であるのに対して,イギリスでは守るべき「利益」ではあっても,権利として客観化されていない（客体視するのではなく関係性の中で評価する）ことが特徴である.この考え方は,利益型の情報に直接適用可能であるばかりでなく,権利型の情報にも（特に,既に知的財産として確立している情報ではなく,新しく生成途上にある概念,例えば著名表示などの表示情報）にも応用可能ではないかと思われる.

最後に第 3 点目として,情報の自由な流通を担保するためには,その媒介者であるコモン・キャリアや ISP,あるいはサーバの管理者などの役割が高まらざるを得ないことを指摘し

ておきたい.わが国ではプロバイダ責任制限法の制定をもって[34],この問題は一段落したかの安堵感が漂っているが,system administrator の役割は,より高くなることはあっても低くなることはあり得ないと思われる(Hardy [1994]).

現に,著作権の分野における,いわゆる「カラオケ法理」「ジュークボックス法理」の議論は,侵害主体の問題(歌唱をする客の侵害行為か,管理・支配するカラオケ店で歌わせる店の侵害行為か)としてではなく,情報の仲介者による教唆・ほう助の問題として扱うべきであろう(前田 [2013]).

また同様に,意に反する情報の流通を差止めようとする場合は,差止命令を仲介者宛に出してもらうことができるか否かは,大問題となろう(中村 [2014]).このように情報社会における情報仲介者の役割については,今後の更なる検討が必要かと思われる.そしてこの指摘は,通信の秘密について述べたところと,関係する面が多いと思われる(インターネットと通信の秘密研究会 [2014]).

参考文献

[1] 池田信夫・林紘一郎 [2002] 「通信政策:ネットワークにおける所有権とコモンズ」奥野・竹村・新宅(編著)『電子社会と市場経済』 新世社

[2] インターネットと通信の秘密研究会 [2013]「インターネット時代の『通信の秘密』再考」(2013 年 6 月)http://lab.iisec.ac.jp/~hayashi/610REPORTIII.pdf

[3] インターネットと通信の秘密研究会 [2014] 「インターネット時代の『通信の秘密』各国比較」(2014 年 5 月)http://lab.iisec.ac.jp/~hayashi/2014-7-7.pdf

[4] 宇賀克也 [2010]『情報公開と公文書管理』有斐閣

[5] 宇賀克也・長谷部恭男(編)[2012]『情報法』有斐閣

[6] 江口佳実 [2010]「英米法によるカンタン法律文書講座」 http://www.hicareer.jp/trans/houritu/index12.html

[7] クリエイティブ・コモンズ・ジャパン [2005]『クリエイティブ・コモンズ』NTT 出版

[8] 宍戸常寿 [2013]「特定秘密保護法案の核心」『世界』2013 年 12 月号

[9] 情報保全システムの関する有識者会議 [2011]「特に機密性の高い情報を取り扱う政府機関の情報保全システムに関し必要と考えられる措置について(報告書公表版)」2011 年 7 月 1 日 http://www.kantei.go.jp/jp/singi/jouhouhozen/dai2/siryou3.pdf

[10] 青弓社編集部 [2004]『情報は誰のものか？』青弓社

[11] 曽我部真裕 [2014]「『情報法』の成立可能性」長谷部恭男ほか(編)『現代法の動態1. 法の生成/創設』岩波書店

[12] 田川義博 [2013]「インターネット利用における『通信の秘密』」『情報セキュリティ総合科学』Vo.l. 5

[13] 田中嘉彦 [2003]「英国における情報公開―2000 年情報自由法の制定と意義―」『外国の立法』2003 年 5 月号

[14] 土屋大洋 [2007]『情報による安全保障』慶應義塾大学出版会

[15] 内閣官房「特定秘密保護法関連」サイト [2014] http://www.cas.go.jp/jp/tokuteihimitsu/index.html

[16] 永野秀雄 [2012]「米国における国家機密の指定と解除―わが国における秘密保全法制の検討材料として―」『人間環境論集』Vol.12, No.2

[17] 永野秀雄 [2013]「国家安全保障及び公共の安全にかかわる情報と情報公開ー米国法(情報自由法)の分析とわが国への示唆―」『人間環境論集』Vol.13, No.1

[34]「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情報の開示に関する法律」平成 13 年法律 137 号

[18] 中村伊知郎 [2014]「権利・利益の侵害と救済手段のあり方：二つの eBay 判決を手掛かりにして」『情報ネットワーク・ローレビュー』(近刊予定)
[19] 西垣通 [2004]『基礎情報学：生命的組織のために』NTT 出版
[20] 西垣通 [2008]『続・基礎情報学：生命から社会へ』NTT 出版
[21] 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)『情報化と経済システムの転換』東洋経済新報社
[22] 林紘一郎 [2003a] 「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
[23] 林紘一郎 [2003b]「情報財への権利付与：経済効率・社会的公正」『計画行政』26 巻 4 号
[24] 林紘一郎 [2005a]『情報メディア法』東京大学出版会
[25] 林紘一郎 [2005b] 「「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」『富士通総研研究レポート』富士通総研経済研究所 No.243
[26] 林紘一郎 [2009]「『個人データ』の法的保護：情報法の客体論・序説」『情報セキュリティ総合科学』Vol.1
[27] 林紘一郎 [2010] 「著作権 (著作物) と Property, Property Rule, そして Property Theory」『アメリカ法』2010-1 日米法学会
[28] 林紘一郎 [2011a]「法学的アプローチ」日本セキュリティマネジメント学会監修・松浦幹太編著『セキュリティマネジメント学』,共立出版
[29] 林紘一郎 [2011b] 「情報法の客体論：「情報法の基礎理論」への第一歩」『情報通信学会誌』Vol. 29, No. 3
[30] 林紘一郎 [2012]「Privacy と Property の微妙なバランス： Post 論文を切り口にして Warren and Brandeis 論文を読み直す」『情報通信学会誌』Vol. 30, No. 3
[31] 林紘一郎 [2013a]「IT リスクに対する社会科学統合的接近」佐々木良一(編著)『IT リスク学：情報セキュリティを超えて』共立出版
[32] 林紘一郎 [2013b]「『個人データ保護』の法益と方法の再検討：実体論から関係論へ」『情報通信学会誌』 Vol.31, No.2
[33] 林紘一郎 [2013c]「セキュリティを管理する：法学的アプローチの役割と限界」『日本セキュリティマネジメント学会誌』Vol.27, No.3
[34] 林紘一郎 [2013d]「通信の秘密：個人の権利か,事業者の義務か」『警察学論集』 Vol.66, No.12
[35] 林紘一郎 [2014]「サイバーセキュリティと通信の秘密」土屋大洋(編)『インターネットとサイバーセキュリティ』角川学芸出版(近刊予定)
[36] 林紘一郎・田川義博 [2012]「心地よい DPI (Deep Packet Inspection) と程よい通信の秘密」『情報セキュリティ総合科学』第 4 号
[37] 秘密保全のための法制の在り方に関する有識者会議[2011]「秘密保全のための法制の在り方について(報告書)」2011 年 8 月 8 日
http://www.kantei.go.jp/jp/singi/jouhouhozen/dai3/siryou4.pdf
[38] ゲーリー・ベッカー,リチャード・ポズナー(鞍谷雅敏・遠藤幸彦訳) [2006]『ベッカー教授・ポズナー判事のブログで学ぶ経済学』東洋経済新報社
[39] 前田陽一[2013]「著作権の間接侵害と民法理論」『著作権研究』No.38
[40] Calabresi, Guido, and Douglas Melamed [1972] 'Property Rules, Liability Rules and Inalienability: One View of the Cathedral' "Harvard Law Review," Vol.85, No.3
[41] Hardy, Trotter [1994] 'The Proper Legal Regime for Cyberspace,' "University of Pittsburgh Law Review," Vol. 55, No. 3
[42] Lessig, Lawrence [2000] "CODE and Other Laws of Cyberspace," Basic Books
[43] Richards, Neil M. and Daniel Solove [2007] 'Privacy's Other Path: Recognizing the Law Journal," Vol. 96, No.2
[44] Murray, Andrew [2014] "Information Technology Law (2nd ed.), " Oxford University Press