製造業における情報管理について

Information Management for Manufacturing Industry

知的財産室
小川哲夫
Tetsuo
Ogawa

総説・解説

1. はじめに

製造業にとって知的財産[注1)]は、企業競争力の源泉であり、企業価値の向上に繋がるものである。一方、知的財産は、「もの」とは異なり「財産的価値を有する情報」であるため、模倣が容易であるという特質をもっている[1)]。近年、こうした知的財産としての技術情報が企業から漏洩する事案が顕在化している。例えば、国内大手半導体メーカーのフラッシュメモリに関する技術情報が業務提携先の技術者によって海外メーカーに漏洩した事案は、賠償請求額が1000億円台の高額であり、刑事事件として逮捕者が出たためマスコミに大きく報じられた。技術情報に限らないが、サイバー攻撃[注2)]による政府機関や企業からの情報漏洩も続発している。

このような不正行為による漏洩に限らず、ヒューマンエラー[注3)]や管理の不徹底から発生するものも含めて、技術情報の漏洩は企業競争力の低下や企業に蓄積された信用（ブランド）の失墜を招くおそれがある。

一方、文書管理システム（本報ではデジタル化した情報を格納・管理するコンピュータ上のシステムを指す）は、デジタル化された大量の技術情報をサーバに保有し、社内ネットワークを介して共有化することにより、知的財産を生み出すための情報基盤として、今やなくてはならないものになっている。また、インターネットやデジタル情報端末は日常生活だけでなく企業内の業務にも普及している。こうした電子情報技術の利便性を損なうことなく、情報漏洩を防止できる情報管理体制とシステムを構築し運用することは、製造業が繁栄を続けるための重要な課題である。

弊社においても、技術情報管理に関する改善への取り組みは継続的に行われているが、本報では、知的財産としての技術情報の管理方法をできるだけ一般的な観点から整理し、技術情報管理のあり方の方向性を検討することとする。

2. 企業内の技術情報と漏洩のパターン

情報技術が発達して、おおむね1990年代末にはインターネットや情報検索システムによって多種多様の公開情報を容易に入手できるようになった。こうして集めた大量の情報から必要なものを選択し体系化した情報や社内独自の知見を体系化した情報は、考察やディスカションなどを経て、技術や経営の課題解決に繋がる高次元の情報になる。一方、こうした情報は、関与した人の知識や知恵へと変化していく。

製造業においては、実験データから高次元の設計情報や製造情報、さらには技術思想に至る様々の技術情報が、社内の文書管理システムまたは紙媒体や人に蓄積されている。また、製造業の重要技術に関する知識や知恵がいわゆる「暗黙知」として、ベテラン従業者のなかで代々企業内に受け継がれている場合もある。こうした「暗黙知」[2)]の後進への継承が近年のM&Aや効率化等の業務環境の変化によって困難になってきたため、「暗黙知」をマニュアル化することによって「形式知」化し、デジタル化を経て社内情報として共有化を進めて管理している企業も多いと考えられる。

さらに、社内で開発された技術だけでは、製品に係わる全ての技術を賄うことができないため、自社にない独自技術に強みを持つ他社とのアライアンスを強化して、新製品を開発する企業も多い。この場合、秘密保持契約に基づく他社からの技術情報や共同の成果物に関する技術情報は、他の社内情報とは、切り離して管理される。

以上述べたように企業には様々の技術情報が存在し、人を介して収集、加工、伝達、管理される（このような行為を本報では「情報行為」[3)]と記す）。情報管理の観点からは、このような情報行為にヒューマンエラーが生じたり、情報行為を行う人に悪意があれば、技術情報が漏洩するリスクが高まるものと考える。平成25年11月に行われた経済産業省産業構造審議会の資料に載せられていた技術流出のパターンを**図1**[4)]に示す。

技術情報漏洩の実態については、2013年度に経済産業省がアンケート調査[5)]を企業に対して行っており、回答全体の13.5%に漏洩があった、70.3%が情報漏洩事例はないと回答している。「中途退職者（正規社員）による漏洩」が含まれていると回答している割合が最も高く50.3%となっている。次いで、「現職従業員等のミスによる漏洩（26.9%）」、「金銭目的等の動機をもった現職従業員等による漏洩（10.9%）」となっている。このように情報漏洩は企業内部からのものが多い結果となっている。悪意のある情報行為による漏洩は秘密裏に

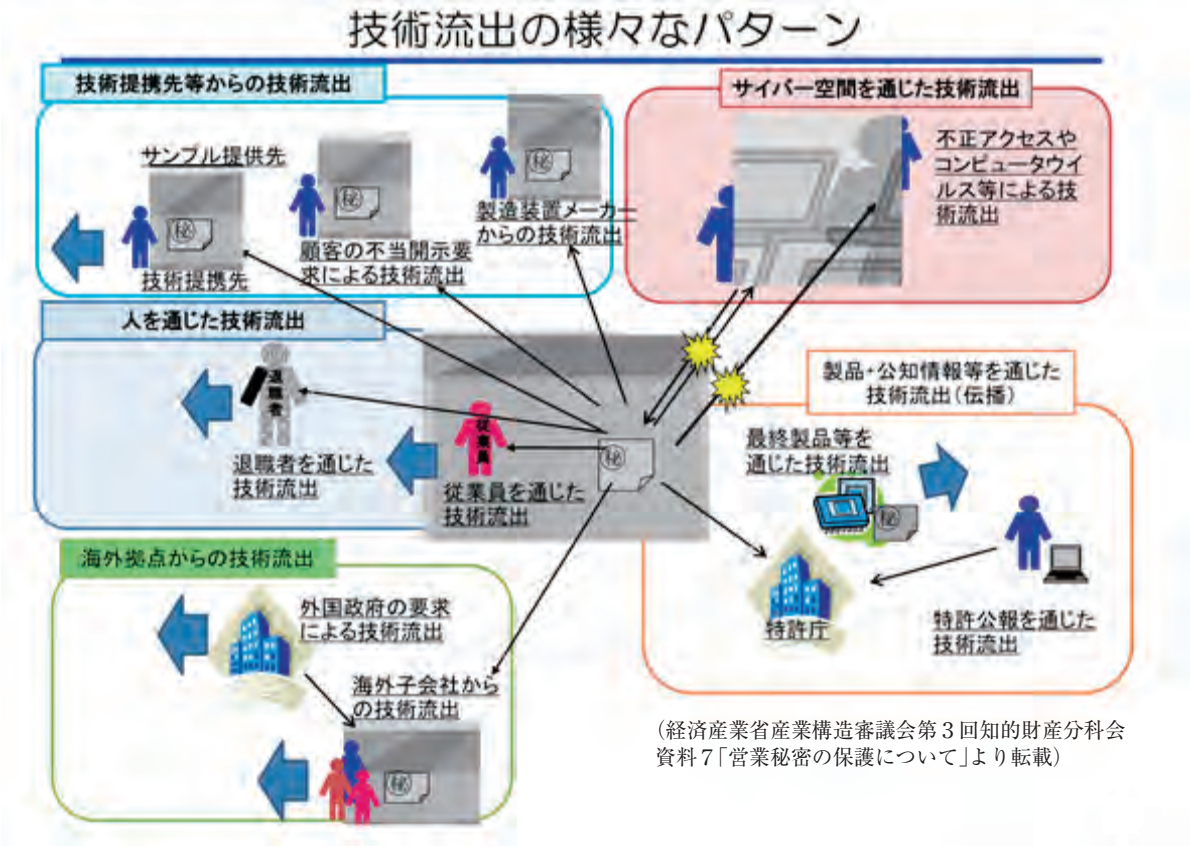


図１　技術流出のパターン

行われることやヒューマンエラーによる情報漏洩は故意ではないことを勘案すると、情報漏洩事例はないと回答した企業のなかにも情報漏洩のあったこと自体に気づいていないケースがあるかもしれない。

3. 技術情報管理

開発業務で生まれた知的財産としての技術情報は、通常、営業秘密として秘匿するか、または特許や実用新案などの知的財産権として守るか、のどちらかを選択することになる。知的財産権の一つである特許権は、技術を公開する対価としてその技術を一定期間、独占排他的に実施することができる権利である。しかし、技術情報の公開によるデメリットも想定されるため、特許請求項における構成要件が他社による権利侵害を検出できる内容になっているか、権利化の可能性や権利化可能な技術的範囲はどれくらいか、競合他社に技術的気付きや市場ニーズなどのヒントを与えることにならないか、などを総合的に検討した上で出願を判断する必要がある。このような判断基準の一例を独立行政法人　工業所有権情報・研修館のウェブページから引用し、以下に記す[6]。

＜ノウハウと特許出願の基準＞

①物と製法の区別 → 製法はノウハウとして秘匿の方向

②侵害発見可能性 → 製品などから侵害発見が困難である場合はノウハウとして秘匿の方向

③他社の到達困難性 → 他社が到達困難と判断する場合はノウハウとして秘匿の方向

なお、この例において、ノウハウは社内ルールに従って一定の書式や資料にまとめて公証役場で確定日付を付してもらい、先使用権の証拠として保管することが記されている。

権利侵害の検出が困難な技術や、他社が到達困難と判断される技術は、上記の例ではノウハウとして秘匿しておく方向が示されているが、こうした判断基準は各社様々のようである。

社内の技術情報をノウハウとして秘匿することを選択した場合、不正競争防止法における「営業秘密」として、適切に管理をしておくことが望ましい。

営業秘密について次章で述べるが、営業秘密は法律上保護される利益に係わる知的財産権として分類されることもある[7]。特許庁ウェブページ上の、営業秘密を含む知的財産権の種類を表したものを**図2**[8]に示す。

4. 営業秘密と法的保護

企業には第2章で述べたように多様な情報が存在するが、不正競争防止法における「営業秘密」は、これらの情報のうち、下記の①～③の要件を満たすものであり（**図3**）[9]、この三要件を満たすことが法に基づく保護を受けるために必要となる。

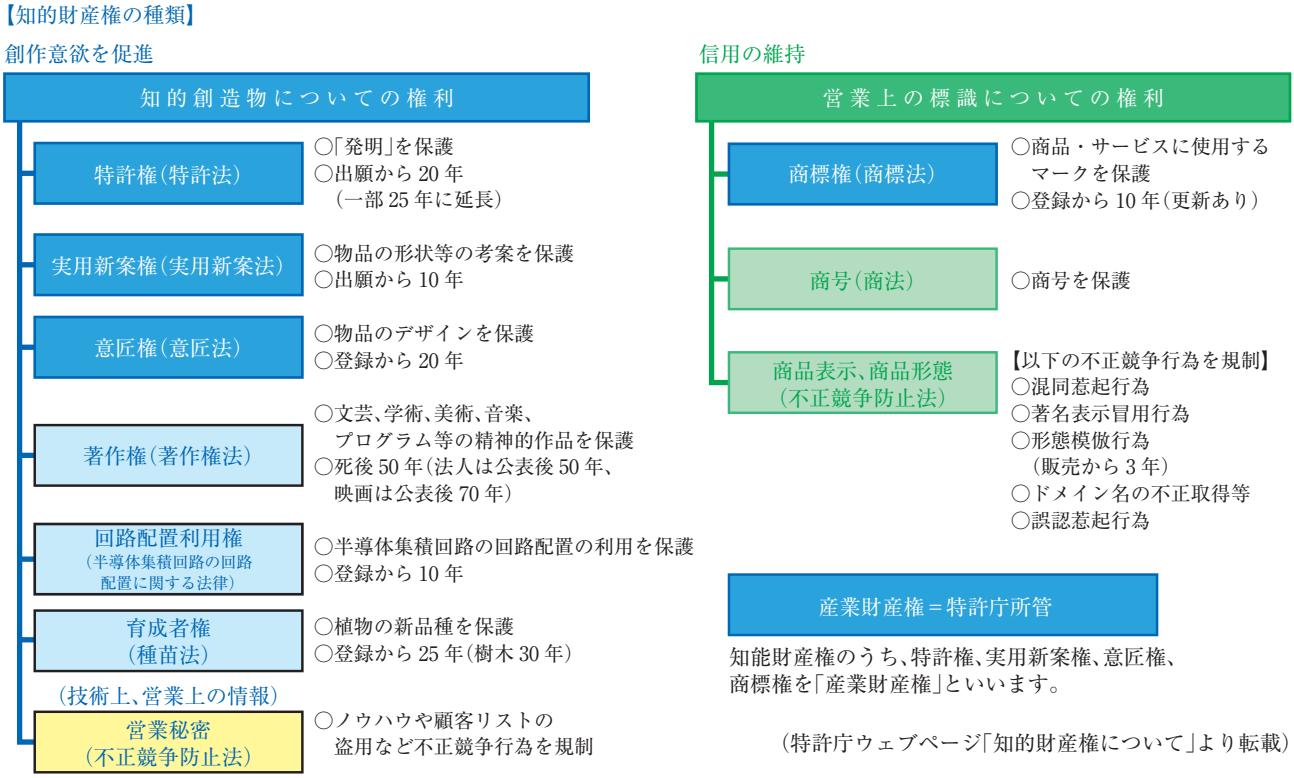
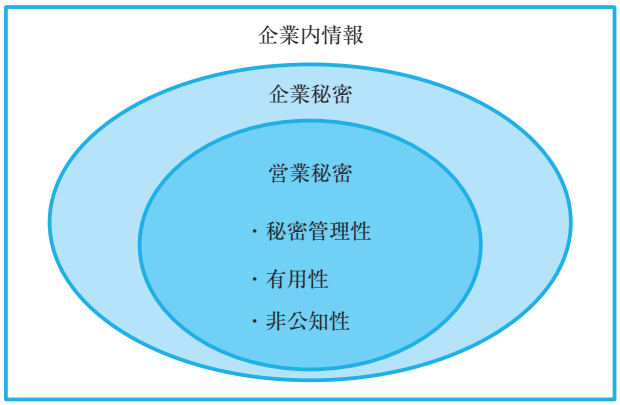


図２　知的財産権の種類



（経済産業省ウェブページ「営業秘密の不正な持ち出しは犯罪です！」より転載）

図３　企業秘密と営業秘密の関係

①秘密として管理されている［秘密管理性］
②生産方法、販売方法その他の事業活動に有用な技術上または営業上の情報［有用性］
③公然と知られていないもの［非公知性］

「営業秘密」はマーケティング情報、顧客情報などの営業上の情報だけでなく、実験データや製品設計図等の技術情報も含む広い範囲の情報が対象である。

不正競争防止法は、「営業秘密」に対する侵害行為に対し、民事上の保護措置（差止請求、損害賠償請求、信用回復措置請求）と、刑事上の保護措置（10 年以下の懲役または 1000 万円以下の罰金（またはその両方）を科すこと）とを定めている。

なお、営業秘密侵害行為に対する抑止力強化を目的として、罰金額の引き上げや、営業秘密侵害罪を非親告罪（被害者の告訴を経ることなく公訴を提起できる）とするなど、不正競争防止法の一部を改正する法律案が 2015 年 3 月に提出された。また、技術情報等の漏洩防止に向け、経済産業省や民間業界団体からなる官民戦略会議が 2015 年 1 月に開かれた[10)]。こうした法的保護の強化や官民一体の取組みは、不正による情報漏洩の防止に大きく貢献することが期待される。一方、各企業は一度情報が漏洩すれば、回収や秘密状態の回復はまず不可能であることを認識した上で、自社の課題として従業員一人一人にまで落とし込んだ漏洩防止策を含む管理の実施が必要である。

5. 営業秘密の管理

社内の技術情報を不正競争防止法における営業秘密として法的保護を受けるためには、前章で述べたとおり、「営業秘密の三要件」を満たす必要がある。そのことをふまえた上で情報管理について、（1）物理的、技術的側面、（2）人的側面、（3）管理体制面から整理する。ただし、「営業秘密の三要件」を満たす具体的な情報管理は、裁判例からも事案毎に要件が判断されており、業容、規模、情報の種類等の事情によって情報管理のあり方は様々であるため、一般解はないと思われる。過去の裁判において要件のひとつである「秘密管理性」が認められないケースが多く[注4)]、秘密管理性の認定が厳しいとの指摘があることをふまえて「営業秘密管理指針」（経済産業省）が 2015 年 1 月 28 日に全面的

に改訂された[注5)]。このような状況であることから、本章で述べる情報管理の事例はあくまで参考としていただきたい。

また、秘密管理性を満たす情報管理だけでなく、企業実務として具体的な情報行為に着目した管理については、**5.4節**で述べる。

5.1 物理的、技術的側面からの管理

営業秘密の要件の一つである「秘密管理性」は、情報へアクセスする従業員を制限すること（アクセス制限）、アクセスした者が客観的に秘密であることを認識できるようされていること（認識可能性）の2つが判断の要素となる。

社内のほとんどの技術情報は電子ファイル化されているものの、情報の種類によっては便宜上、秘密情報を含む紙媒体をファイリング保管している企業は多いと思われる。これらは「社外秘」等の表示を基本とし、施錠のかかるキャビネットへの保管が必要となる。

また、文書管理システム上の営業秘密に相当する電子ファイルを印刷できなくする仕組みや、秘密として管理している情報であることを表す表記を自動的に紙媒体等に印字する仕組みも秘密管理性の観点から有効と思われる。

営業秘密を含む上記技術情報を入手できる場所へは、社内関係者以外が立ち入れないようにすることが基本である。関係者以外の入室を禁じる表示やルール化だけでなく、指紋やセキュリティカードによる認証システムを採用して入室できる人を制限することも必要であろう。

また、従業員のIDによりアクセス権限を区分して、例えば他部門のサーバや特定の文書管理システムへのアクセスを制限している企業は多いと思われるが、情報の管理と共有化との両立の観点から、情報共有を目的とするサーバを設置して、情報の種類や重要度に応じてアクセス権を個別に付与して運用することも必要であろう。

上述の他、社外へのデータ持ち出しや電子メールによる社外への情報発信などを、情報管理責任者（**5.3.2**を参照のこと）による許可制にすること、電子メールによる情報量を制限すること、特に重要度の高い情報は一切の持ち出しを禁じ、紙媒体への印刷を操作上不可能にすること、電子情報はログ管理することなどが、アクセス制限と認識可能性の措置とあわせて、秘密管理性の観点から有効である。

5.2 人的管理

一般的に以下の対処が挙げられる。

5.2.1 秘密保持誓約書

新入社員や中途採用者等とは法的な担保として、入社時に秘密保持誓約書または契約書を締結しておく[11)]。

5.2.2 教育（周知）

技術情報管理規程、ガイドライン等を、従業員へ周知し、実行するよう定期的な教育や研修を行う[11)]。営業秘密の漏洩に関する判例では、教育・研修が実施されていることは、情報の秘密管理性の認定の決定的な要素ではないが、教育・研修・啓蒙などを日常業務のなかで、意識的に行うことが望ましい。

5.2.3 中途採用者への確認

中途採用者に対しては、前職で負っていた秘密保持義務や競業避止義務の存在の有無を確認し、中途採用者が持ち込む情報に法的リスクはないか等を確認しておく。

5.2.4 競業避止義務契約

定年退職または中途退職者と競業避止義務契約を締結し、退職後は一定期間競業会社に就職しないという契約をすることが一般に行われる。しかし、義務期間が長すぎるなど、退職者に過度の競業避止義務を課すことは、憲法で保障する「職業選択の自由」の侵害になるため、契約自体が無効とされる可能性がある[12)]。また、中途退職を表明した人を社内秘密情報から技術的・物理的に遮断するなど、適切な処置が必要である。この種の漏洩防止には、在職中における良好な人間関係や従業員へのインセンティブの配慮等が有効と考えられる。

5.3 管理体制面

リスクマネジメント方針や情報管理方針などの上位方針に従って情報管理規程やガイドラインが作成され、それらが従業員に周知され、営業秘密を含む情報管理を実現可能とする組織体制化が、企業内の組織実態をふまえた上で行われることが望ましい。

5.3.1 情報管理ガイドラインの作成

情報漏洩のリスクが何処で、何時、どのような情報行為や行動において発生するのかを十分に検討した上で、ガイドライン（または規程）を作成する必要がある。ガイドライン作成の準備としては、社内技術情報から営業秘密として管理するべき情報を特定して一般情報との区分を明確にしてから、棚卸しを行うことが推奨される[13)]。ガイドライン作成の一例として、営業秘密に相当する情報をいくつかに分類したリストを作成し、営業秘密管理の三要件の観点から課題を抽出、個々の課題に対して実行可能な対策を検討して、検討結果をガイドライン等のルールに反映させることが挙げられる。

技術分野や情報の種類にもよるが、情報リストの分類が細かすぎると、木を見て森を見ずの作業になるため、営業秘密として管理する視点から最低限必要と考えられる程度の分類でも良い場合があると考える。

また、これらの情報は重要度のランク付けを行い（例えば、社内でも特定の人のみがアクセスできる情報、社外には絶対に出さない情報、契約や特許等の対象としてよい情報、交渉や技術交流のために社外に出してもよい情報等）、ランクに応じた管理方法をガイドラインに示しておくと良い。

営業秘密の管理に関する上記課題の対策は、各部署の情報行為の実態を把握した上で、文書管理システムの利便

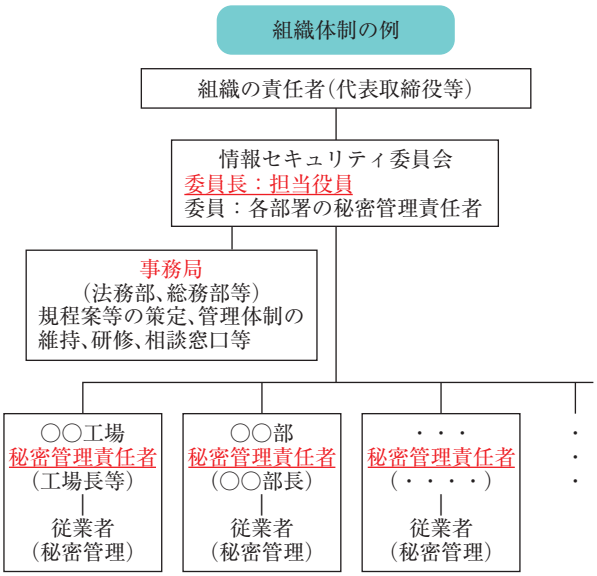
性をできる限り損なわずに実施できるように検討することが重要である。

アクセス制限については、細かく設定した場合に、毎年度の組織変更や人事異動、昇格による権限の変化への対応の工数が問題となる。アクセスを制限する意義を十分に議論しておかなければ、セキュリティ対策工数や費用が大きくなってしまうことに留意するべきである。

5.3.2 組織体制

企業内の情報管理体制については、各部門の秘密管理責任者（情報管理責任者）を定め、その管理責任者から構成される情報セキュリティ委員会を設置し、情報管理に関わる実務を担う事務局を上記委員会に属する組織図が、経済産業省知的財産政策室による「営業秘密管理（実践編）」のなかで提案されている（**図4**）[11]。

情報管理体制のあり方は企業事情により異なるが、こうした体制が形骸化しないように、意義のある組織行動が継続的に行われる仕組みを作っておくことが重要と思われる。



（経済産業省ウェブページ「営業秘密管理（実践編）」より転載）

図４　営業秘密管理の組織体制の例

5.4 情報行為に着目した情報管理

公知情報を集めて整理・加工・分析したものや、その情報から得られた考察を記した情報は、秘密情報として扱うことが基本である。このような情報は多大な工数と費用をかけて作成する場合もあり、作成者が認識する以上に企業戦略の方向性などを示唆する内容を含むことがある。こうした情報を社外のプレゼンテーションに使用する場合は、開示する情報の範囲を限定し、情報管理の責任者による許可制とすることが望ましい。

研究や開発段階における仕入れ先からの物品購入では欲しいものを効率よく選定するため、仕入れ先との面談を伴うことがある。このような面談は開発スピードや課題解決にも影響する大切な場であるので、事前に開示できる情報の範囲を確認しておくことや、交渉経験の少ない人は部門責任者を同伴して面談するなどの対処が考えられる。情報に対する意識付けの観点からは、面談記録を作成したり、場合によるが議事録を作成して双方で開示情報を確認することなどが望ましい。

逆に顧客からの情報は、契約がない場合でも将来、契約の範囲内に含まれることを想定して、その管理を社内で徹底させなければならない。情報の開示等を顧客に要求して過多に情報を入手したり、面談における議事録がなかったりすることによって、後になって成果の帰属等を決める際に問題が発生することがある。顧客に限らず、社外の人との面談・交渉する場合は、後に情報のコンタミネーション[注6)]を起こさないために、事前に関係する公知情報の範囲と自社技術の範囲とを把握しておき、顧客からの情報の区分を明確化しておくこと、場合によるが自社開発技術などを含む資料を公証役場で確定日付を得ておくことも有効と思われる。

契約に基づく他社からの秘密情報については、社内の他の情報と物理的にも隔離し、アクセス制限など厳重な管理が必要である。このような契約は法的強制力を持つ企業間の約束であることを従業者全員に周知しておかなければならない。社外への秘密情報の持ち出し、ノートパソコンやタブレット等のモバイル通信機器の社外での操作、学会発表、企業団体や学術団体における交流会などの社外での情報行為は、予期せぬところで技術情報漏洩に繋がることがある。また、社内での営業秘密の廃棄方法のルール化、個人USB使用の原則禁止、撮影や録音禁止、社外からの実習者との秘密保持契約等について、規程やガイドラインで文書化しておくだけでなく、定期的な社内教育や啓蒙活動によりルールに基づいた情報行為と情報倫理を社内に定着させることが、より優れた情報管理を実現し、社会的信頼を築く観点から重要と考える。

6. 漏洩防止と共有化との両立

最近は多くの優れた文書管理システムが販売されているので、これらの選択と企業環境に適合した作りこみは、情報のセキュリティ向上と社内共有化との両立という課題の改善に有効と考えられる。

製品やその製品の配合、製造工程表等の技術情報については、これらの情報を共有すべき関係者を特定できるので、厳密なアクセス権限の設定が有効である。

一方、研究や開発過程で生まれた要素技術や、重要技術の本質を表す技術情報は、企業の将来の繁栄や事業のグローバル展開にとって重要である。これらの技術情報は見える化や概念化されることによって、コミュニケーションによる社内共有化を容易にし、新たな製品設計技術等の知的財産に繋がることが期待される。したがって、単にアクセスが可能という意味での共有化ではなく、コミュニケーションによる相互理解を伴う共有化に変える仕組みを作ることと、このような共有化

の障壁とならぬようにアクセス制限等の管理面を工夫することが必要であろう。

7. 海外関係会社における情報管理

工業所有権情報・研修館や経済産業省などのウェブページに海外における技術情報漏洩の実態や、漏洩対策について報じられている。これらの報告のなかには、海外では特に、現地従業員との契約において違反した場合の罰則、損害賠償請求等を定めておくことの必要性が多く記されている。海外では規程やガイドラインは守ってくれるものではなく、守らせるものという認識で、罰則を厳格に適用する必要性や、ローカルマネージャに部下の管理責任や権限を与えること等、国内よりも一層漏洩に対して厳しい対応をしなければならないことが記されている[14)]。また、「TRIPS協定」の加盟国間では、営業秘密の最低限の保護水準を定めていることを現地に周知しておくべきであろう。

しかし、上記のような海外での情報管理は、現地の事情によって必ずしも容易ではないと思われる。また、海外へのビジネス展開は現地関係企業と、目指すべき企業価値を共有する必要があるため、技術情報に限らず多様な情報のやり取りが行われる。特に技術情報については開示可能な範囲を明確にした上で、海外展開に向けた経営の大きな方針に沿った、適切な情報管理のあり方を検討する必要がある。

グローバルに情報を共有し管理するシステムは、海外関係会社のビジネス環境や通信環境にも適合させる必要がある。市場で既に実績のある管理システムの導入や、情報コンサルタント会社等の専門家のサポートの利用は、早期に情報管理システムを構築するには有効であると思われる。他方、グローバルな情報管理方針に基づいた情報管理システムの運用ルールを作り、そのルールに基づいた情報行為を従業員が遵守し継続できる仕組みを作ることも重要である。

8. おわりに

本稿の作成にあたっては、インターネット上の情報を多く参考にさせていただいた。技術情報の管理に関する優れた論説[15)]が多数あるため、社内の情報管理体制を具体的に検討される方は、これらを参考にされたい。

情報の共有化を前提に、企業からの技術情報の漏洩防止を実現する管理システムの構築は困難を伴うが、まずは基本となる社内ルールや体制等の管理基盤を作り、これらを固定化するのではなく、組織変更やM&Aなど刻々と変化するビジネス環境を予測しながら、都度適応して行くことが現実的なやり方であろう。こうした社内ルールを遵守することを前提に、社員一人一人が技術情報の重要性を理解し、情報への感度（重要度と区分を即座に判断し対処できる能力）を向上させることが情報行為における漏洩を防ぐことに繋がるものと考える。悪意のある情報行為に対しては、決して許さない姿勢を企業が示し、そのような行為を生まない風土を育てるために、漏洩は懲戒処分や刑事罰の対象であることを教育のなかで周知するもことも必要であろう。

注記

注1）「知的財産」は知的財産基本法の第2条において『この法律で「知的財産」とは、発明、考案、植物の新品種、意匠、著作物その他の人間の創造的活動により生み出されるもの（発見又は解明がされた自然の法則又は現象であって、産業上の利用可能性があるものを含む。）、商標、商号その他事業活動に用いられる商品又は役務を表示するもの及び営業秘密その他の事業活動に有用な技術上又は営業上の情報をいう。』と規定されており、本稿の「知的財産」も上記の意味で使用する。

注2）不正プログラムを添付した電子メール（標的型メール）を送信し、これを受信したコンピュータを不正プログラムに感染させることによって、被害者の知らぬ間に機密情報を外部に送信させ、情報の窃取を図る標的型メール攻撃が代表的。

注3）ヒューマンエラー：人為的過誤や失敗（ミス）のこと。一般に事故や災害に繋がる行為を指す。人間である以上必ずエラーは起こりうるため、人間に任せる完璧な対応策はないといった観点に基づいた事後や災害防止対策を講じる必要がある。JIS Z8115：2000 G20では、「意図しない結果を生じる人間の行為」と規定する。情報行為においても同様のことが当てはまると考える。

注4）経済産業省による平成25年8月16日改訂版「営業秘密管理指針」の32頁には「営業秘密に関する裁判例のうち、秘密管理性について判断していると考えられるものは81件ある。その中において、秘密管理性を肯定したものは23件である。」と記されており、3割弱程度しか認められていない。

注5）“営業秘密管理指針（平成27年1月28日改訂版）”、経済産業省ウェブページ、http://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html（参照 2015/5/29）、改訂版の指針は「不正競争防止法によって差止め等の法的保護を受けるために必要となる最低限の水準の対策を示すものである」とされ、改訂前の86項を17項にまで大幅に頁数を減らして要点が理解し易く整理された。とは言え、一般従業者が実務の中で、上記指針を理解して三要件を満たす情報管理をイメージして実践するには少し無理があると思われ、専門知識を有する管理部門による対処や指導が望まれる。

注6）経済産業省による最新版 “営業秘密管理指針”（平成27年1月28日改訂）の前の平成25年8月16日改定版には、情報の“コンタミネーション”の防止について記されている（64頁等）。

参考文献

1）“知的財産権について”、特許庁ウェブページ、https://www.jpo.go.jp/seido/s_gaiyou/chizai02.htm（参照 2015/5/29）

2）野中郁次郎:“知識創造の経営”、p.91-92、日本経済新聞社（1990）

3）白井豊:“情報・倫理・知的財産”、p.5、創造舎（2010）

4）“営業秘密の保護について”、特許庁ウェブページ、第 3 回知的財産分科会議事次第、資料7 http://www.jpo.go.jp/shiryou/toushin/shingikai/tizai_bunkakai_03_paper.htm（参照 2015/5/29）

5）“人材を通じた技術流出に関する調査研究報告書（別刷）、営業秘密の管理実態に関するアンケート調査結果”、三菱UFJリサーチ&コンサルティング、(2013)

6）“化学系の企業の実例”、工業所有権情報・研修館ウェブページ、http://www.inpit.go.jp/katsuyo/tradesecret/kanri.html（参照 2015/5/29）

7）石田正康 :“知的財産としての営業秘密”、特許研究、〔42〕、2-4、(2006)

8）“知的財産権について”、特許庁ウェブページ、https://www.jpo.go.jp/seido/s_gaiyou/chizai02.htm

9）“営業秘密の不正な持ち出しは犯罪です！それ大丈夫?（2013 年 3 月）”、経済産業省ウェブページ、http://www.meti.go.jp/policy/economy/chizai/chiteki/（参照 2015/5/29）

10）“技術情報等の流出防止に向けた官民戦略会議”、経済産業省ウェブページ、http://www.meti.go.jp/prss/2014/01/20150128003/20150128003.html（参照 2015/5/29）

11）“営業秘密管理（実践編）（平成25年8月）”経済産業省ウェブページ、http://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html#toriaezu（参照 2015/5/29）

12）“営業秘密保護のための競業避止義務の締結の方法”、経済産業省経済産業政策局知的財産政策室　編、経済産業調査会、(2013)

13）肥塚直人：“「技術流出」リスクへの実務対応”、中央経済社、(2014)

14）“素形材企業のための技術・ノウハウ保護ガイドブック～海外で勝ち抜くために～”、経済産業省ウェブページ、http://www.meti.go.jp/policy/mono_info_service/mono/sokeizai/gizyutsuryusyutsukaitei.html（参照 2015/5/29）

15）・“営業秘密・知財戦略入門～大切な技術情報を守るために” 工業所有権情報・研修館ウェブページ、http://www.inpit.go.jp/content/100584406.pdf（参照 2015/5/29）

・“営業秘密の保護について”、経済産業省知的財産政策室ウェブページ、http://www.jpo.go.jp/shiryou/toushin/shingikai/tizai_bunkakai_03_paper.htm（参照 2015/5/29）

・フェアトレード委員会:“営業秘密管理における実務的課題”、知財管理、**59**[6]、649-668、(2009)

・「営業秘密管理の考え方−営業秘密管理のための手順−」経済産業省ウェブページ、http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/slide2-ver_20.pdf（参照 2015/5/29）