企業不祥事、不正対応の現場～平時に生かす、有事対応の現実～

第1回　「営業秘密」と産業スパイ

デロイト トーマツ ファイナンシャルアドバイザリー㈱ フォレンジックサービス　木原（きはら） 京一（きょういち）

デロイト トーマツ ファイナンシャルアドバイザリー株式会社（以下、DTFA）フォレンジックサービスは、企業のさまざまなリスクへの対処、予防、発見の業務経験を有する企業不祥事を専門とするスペシャルチームである。 例えば、不正・不祥事が発覚した企業に対しては、効果的な事実解明や解決策の提供などによって、社内調査の信頼性を補強するばかりでなく、再発防止策の策定や不正実行者の責任追及等、調査後も企業価値の回復に向けて継続的な支援を行い、不正リスクに有効な内部管理体制構築のアドバイスや内部監査の支援、各種研修サービスも提供している。

本連載では、フォレンジックサービスが経験した企業不祥事、不正対応の現場を紹介しながら、実際の企業不祥事を有事と捉え、有事を想定した平時の運用に生かしていただき、対岸の火事とせず、他山の石として貴社のリスク管理に役立てていただければ幸いである。

ITの進歩で劇的に増加してしまった産業スパイの存在

『産業スパイ』という言葉を聞くと、メディアを賑わすような大事件や、映画・ドラマの世界を想像され、現実の世界とはかけ離れた事象と思われる方も多い。しかしながら、産業スパイが連想させる、ビジネスの世界で暗躍しながら、裏社会と通じ様々な情報戦を繰り広げ、試行錯誤の末に企業の所有する技術や経営情報を待ちだしているというようなイメージとは異なり、現実には、極めて容易かつ頻繁に、企業にとって重大な情報が持ち出され、不本意な形で第三者に渡るケースが起きている。

産業スパイの増加に大きく寄与してしまったのが、ITの進化とIT機器のコモディティ化によるメディア機器等の大容量化と低価格化。また、企業自体が保有する情報が肥大化、ビックデータ化したことで、自社にとって重要かつ機密性の高い情報の管理が大変難しくなっている現実が浮き彫りにされている。

ちなみに、32GB容量USBメモリ記憶媒体（市場価格およそ2,000円）で、500万画素の写真を約3万枚記録する事が可能である。

仮に企業の所有する重要な情報が図面や写真記録だったと仮定した場合、かつてはダンボール何箱にもなってしまい、物理的に持ち運ぶことが困難だった書類が、PDFやTIFFなどといった様々な形式の電子データとして保存・保管され、USBメモリやSDカードといった、掌に収まってしまうサイズにして持ち運ぶ事が出来てしまうのである。

「営業秘密」と改正不正競争防止法、企業が留意すべき重要点

日本企業における重大な情報流出事件は後を絶たず、年商1兆円規模を超える企業における外国人労働者や日本人社員による外国企業への情報提供など、センセーショナルな事件も複数回にわたり起きてしまった。

こうした中、政府は2009年、不正競争防止法の改正案（営業秘密侵害罪における処罰対象範囲の拡大等）を可決し、「営業秘密」の領得自体への刑事罰が導入された。これは、領得行為（他人の物を自己の物のように処分し、もしくは処分できる状態に置くこと）の事実確認がされれば、処罰の対象に含まれるという内容である。

我が国においては、「営業秘密」の管理・流出が大きな問題・課題として浮き彫りになっており、特に経済産業省（以下、経産省）は、この「営業秘密」における企業の管理体制や取り組みを非常に重要視している。

「営業秘密」とは、企業秘密、技術情報、顧客情報、個人情報、従業員情報、IR/PR（経営）情報、R&D（研究開発）情報など、様々な企業の所有する情報の中で、それぞれの企業が自ら特定・指定する機密情報である。

この「営業秘密」という言葉の定義が、企業をはじめ、多くのビジネスパーソンの理解や解釈に個人差を生じさせてしまっている、ややこしい点であるが、この「営業秘密」は不正競争防止法とセットで考えると理解しやすい概念である。我が国、特に経産省では、企業にとって大切な情報を守るために、企業の重要事項、つまり機密事項や秘密事項などを「営業秘密」として定義づけし、管理している。これにより不正競争防止法の適用などを含めた法的な

保護が活用できる。

つまり、企業の所有する、細かい情報内容に対して、国や法律が「営業秘密」と決めるのではなく、企業それぞれが、各々の意思決定で、

① 技術情報
② 顧客情報
③ 経営／財務情報
④ 営業情報
⑤ 研究開発情報

といった、様々なカテゴリから、自社にとって大切な情報を取りまとめ、定義し、そして選択された情報群をその企業の「営業秘密」と設定する。不正競争防止法においては、定義され、かつ決められた運用の下で管理された「営業秘密」に関しては、不正使用などの侵害行為に対して、差し止め請求や、損害賠償などの法的措置をとることが可能となるのである。

企業自らが設定した「営業秘密」に対しては、原則として下記の3要件を満たすことが必要となる。

① **秘密管理性**

対象となる情報／データが「秘密」として管理されていること

※情報のアクセス権限の限定

※アクセス権限のない社員及び関係会社社員が偶然必然問わず、営業秘密情報に接触した際に、当該情報が「営業秘密」である、という事を認識できること

② **有用性**

有用な経営・営業上、又は技術上の情報であること

※有害物質の垂れ流しや脱税等の反社会的な活動については、正当な事業活動ではないため、有用性がある情報とは認められない

③ **非公知性**

公然と知られていないこと

※刊行物等に記載された情報は、営業秘密に値しない

これら、企業の大事な情報を守るために、自社の「営業秘密」を細かく設定・分類・管理することで、技術情報や顧客情報といった、企業の生命線となる情報マネジメント、企業にとっては、より大きな課題である文書管理の着手にもつながる。また、情報流出のリスク低減はもちろんの事、不幸にも不正な流出などが起こった際には、流出してしまった情報が「営業秘密」として、定義・管理されていれば、不正競争防止法に基づき、速やかに法的措置を取る事で不正・不祥事に対して、強い企業イメージをステークホルダーへ印象づける事が可能となる。

人材を通じた技術流出に関する調査研究結果から

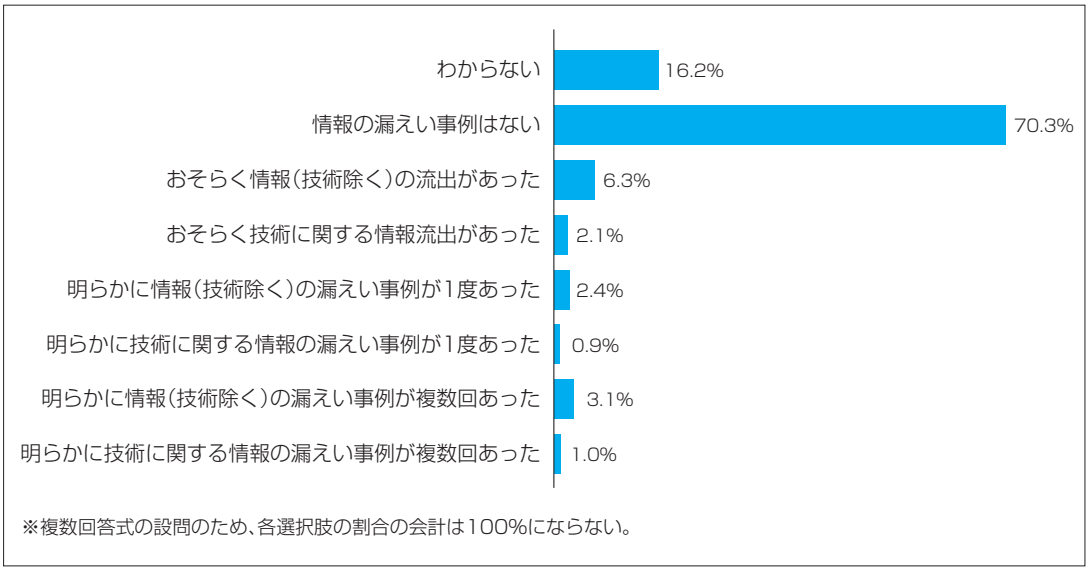
2013年3月、経産省は日本企業1万社を対象に（回答企業約3,000社）「営業秘密の管理実態に関するアンケート調査」を実施し、結果概要を発表した。

注目すべきは、この大規模なアンケートの実施背景である。これには、日本の大手製造業による「営業秘密」の流出により、外国企業を提訴したケースが大きく影響している。我が国では、特許侵害訴訟と併せて、知的財産における、「営業秘密」の管理・流出が大きな問題・課題であることが国策としても認識されている。

このレポート調査研究結果によると、役員、従業員、転退職者、取引先、派遣社員等、人を通じた過去5年間での営業秘密の漏洩事例の集計をした結果、13.5%の企業がなんらかの営業秘密情報の漏洩を経験している。

＊1 経済産業省Webページ
http://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html

図表1　過去5年間での営業秘密の漏えい事例

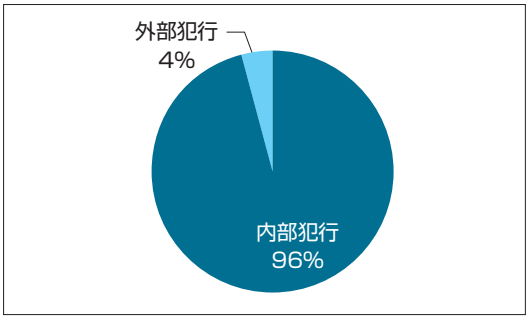


（出典）平成24年度「人材を通じた技術流出に関する調査研究報告書（別冊）『営業秘密の管理実態に関するアンケート』調査結果」（経済産業省）50ページ

調査事例にみる内部犯行の割合

DTFAにおいて、2011年から2013年にかけて調査した情報漏洩（「営業秘密」問わず、すべての情報漏洩事故）調査を行った内容を、外部犯行と内部犯行で分類した結果、当社の調査事例においては、96%もの割合で、内部による不正実行であったことがわかった。直接的に「営業秘密」に関与できない人物も、間接的あるいは別の社内関係者を通して、といった手法で機密情報にアプローチする手段を講じることが難しくない。企業の大小に関わらず、内部実行犯への対策はあらゆる組織で必要である。

図表2



さて、ここからはDTFAで行った、実際の不正対応・調査事例をご紹介する。実際に企業で起きている事象を参考にしていただき「営業秘密」という概念を自社に置き換える、あるいは情報マネジメントの管理を再考する参考にしていただければ幸いである。

事例　「何を盗まれたのかがわからない」

大手製造業のA社に極めて重大な技術情報漏洩の疑いが発生したのは、まさに晴天の霹靂であった。

ドイツ支社に駐在するスタッフから、緊急で役員に報告が入ったのである。

ドイツ駐在スタッフからの報告は要約すると下記の通り。

現在、フランクフルトでは国際的な展示会が開かれており、当社（A社）も出展しているのだが、A社にとって最も大きな得意先であるX社より、『X社とA社にとって極めて重大かつ機密性の高い情報が漏れている』という報告を受けた。その内容は、A社の競合である、B社の展示ブースにおいて、X社と協同で開発したA社の次期主力製品とほとんど同じ内容、コンセプトのプレゼンテーションが行われていた、というものであった。

さらに、展示会場でB社のプレゼンテーションを観ていたX社の担当によれば、数ヶ月前にA社がX社にプレゼンした内容と極めて似通ったスライドや図を用いられており、定量的な数値説明には、X社側が提供した情報も数多く混在していた、という内容だった。

X社側はA社に対し、事実関係の究明解明を至急依頼すると共に、当面の取引及び技術提携関係の凍結を示唆。4月後半の出来事で、大型連休を控え、製造業にとって大変な繁忙期を迎える前に起きてしまった緊急事態だった。

※グローバル企業にとって、日本に限らず各国のカレンダー把握は非常に重要である。世界的なビジネスにおいて経験の浅いA社にとっては、業務管理のバランスが日本国内に集中しがちとなり、4

月中盤のこの時期、つまり大型連休を控えた長期休業前に生産ライン調整や国内顧客対応で連日150%稼動に近い状況にあった。

数日間のA社総出による調査の結果、情報漏洩の根本的原因は数ヶ月前の12月末に、両親介護を理由に九州の実家へ帰ると言い残して退職した企画・デザイン課長αであろう、という結果となった。社員へのヒアリングでαが数名のA社在籍同僚へ、B社への転籍を話したこと、ドイツでの目撃情報など、複数の状況証拠が揃ったことから、A社は判断した。一方で、αは企画系の社員であり、退社以降もA社としては、それほどのリスクを考慮していなかったが、「営業秘密」のアクセス権において、A社では主要な課長職はほぼ全社の資料を閲覧、ダウンロードが可能であり、また誰が閲覧し持ち出しを行ったか、という履歴を追うことが出来ない運用であることも経営陣は知ることとなった。A社は、被疑者の特定までには至ったものの、そもそも、何をされ、何を持ち出され、今後もどういった影響が自社に及ぶかを、全く把握出来ないという状況に陥ってしまったのである。

被疑者の特定までの数日間、関われる人材の全てを費やし、企画・デザイン課長αまでたどり着いたA社であったが、すでに自社での調査はリソースとスキルにおいて限界に達しており、また、世界的グローバル企業X社の求めるレポートに対応できる能力は残っていなかった。

もちろんA社は製造業界において優良企業であり、製品及び社風においても国内外で一定の評価があった事で、グローバル企業への成長を果たした。しかしながら、クロスボーダーの取引においては、相手方はA社の平時運用においてこのような事態に対応することを要求する。今後の企業成長において、A社は内部統制の構築や内部監査基準の整備を進めていかなければならない。

ケーススタディ　事例　A社から学ぶべきこと

1. マネジメント層（部課長といったミドル）の活動履歴管理と人物評価
   ※マネジメントの退職離職を安易に捉えず、リスクを鑑みた対応を。
2. 部課長に与えられた権限の確認と見直し
   ※課長や部長に対する一律アクセス権限などの合理性を見直す。例えば、本ケースでのデザイン系の課長職が、R&Dに関わる新規事業開発までリアルタイムで把握でき、かつR&D部門サーバーまでアクセス可能である必要があったのか。
3. 「営業秘密」の定義が曖昧
   ※A社が管理している情報の整理、分類を実施していなかった為、社内における重要情報や機密事項の判断、解釈が属人化してしまい、企業内個人の判断·価値観が優先されることとなった。つまり、役職者やマネジメント層の不正の温床になりやすい（機会の提供）。
4. 不祥事対応時の情報管理
   ※連休を目前に控えた緊急事態とはいえ、情報漏洩に関連した社内調査において、事実関係がはっきりわかっていない状態で、調査スタッフの数だけ増員することは、被疑者に内通している者へ企業側の情報が渡りやすくなることや、マスコミやステークホルダーなど、外部へのリークが発生する等の非常に大きなリスクとなる。
5. 事実関係の把握が難しい会社
   ※ここ何年かで、有事対応の企業力が問われており、有事における企業が出来得る、最短かつ最も必要とされている事とは、『何が起きたのか？どのようなご迷惑をおかけし、何が出来るのか』に集約され、わかりやすく言い換えれば、事実関係の把握がすぐに出来るか否かで外部の評価は変わる傾向がある。

A社で起きた事は、ドラマや小説の世界、あるいは限られた企業にしか起こらない事象ではなく、グローバルに展開を図る企業であれば、相応に起こりうる潜在的なリスクである。今回のテーマに挙げた「営業秘密」という概念は、企業100社あれば、100通りの「営業秘密」が存在する事を認めた上で、企業側が自社の情報を自ら率先的に整理・分類し、「営業秘密」の定義に則った管理運用を行うことで、平時の抑止から有事の速やかな対応、法的なサポートも可能にする、企業にとっては極めて有効な定性的手法である。

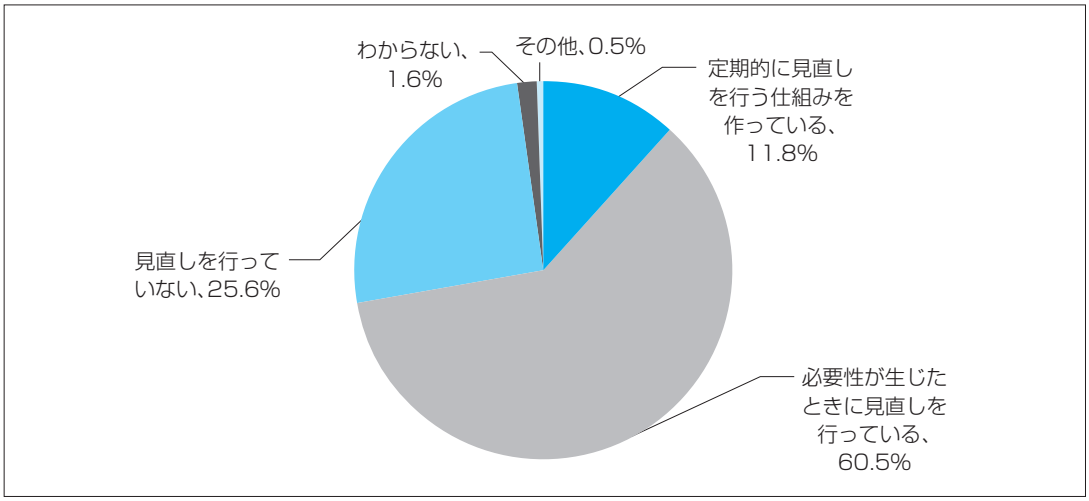
経産省のWebサイトでは、様々な情報がアップデートされており、この機会にこういった当局の無償かつ有用な情報をご利用されることを推奨する。

最後に、人材を通じた技術流出に関する調査研究結果から、「営業秘密」の区分と格付けの見直しについてのアンケート結果も下記に添付する。成長企業における情報はナマモノに等しく日々価値や中身が変わる無形資産であり、その中で企業における有用な情報定義が儀式的に最初に1度だけ決める格付け行為であっては、せっかく選定した「営業秘密」も形骸化する恐れがある。

企業のコアコンピタンスに関わる重要な技術、顧客情報に関しては、定期的に整理・分類・更新するシステム、つまりPDCAサイクル運用も併せて実施願いたい。情報の定義以上に、難しく体力の必要な作業であり、相応の負荷が伴うが、大事なポイントは合理的に作り上げたシステムを無理なく、永続

的に継続運用するかである。

図表3　営業秘密の区分と格付けの見直しについて



（出典）平成24年度「人材を通じた技術流出に関する調査研究報告書（別冊）『営業秘密の管理実態に関するアンケート』調査結果」（経済産業省）6ページ

以　上

