営業秘密漏えいリスクとその対策

製品の製造方法、顧客情報データ、商品の購買情報等の営業秘密は企業の財産であり、競争力の源泉である。また昨今では機械学習や AI 等の技術の進展によるビッグデータの利活用を進めている企業も増え、情報の重要性はますます増加している。一方で、近年は内部犯による犯行を含め営業秘密の漏えいに関する事件が数多く発生しており、企業は営業秘密の保護対策を一層強化する必要がある。

本稿では、営業秘密漏えいリスクの実態と企業が講じるべき対策について解説する。

1．営業秘密漏えいリスクの実態

（1）多発する営業秘密漏えい

2012 年 4 月に鉄鋼メーカーA 社が、自社の製造技術に関する営業秘密が不正に取得・使用されたとして、韓国の競合大手企業と情報を流した A 社の元従業員を提訴した。また 2014 年 3 月には、B 社の提携先半導体メーカーの元技術者が、転職先の韓国競合企業に B 社の研究データを提供した疑いで逮捕された。更に同年 7 月には、C 社の大量の顧客情報が、システム運用を行っている業務委託先の元社員によって不正に持ち出され、名簿業者に売却されたことが発覚した。これらの大型事件の続発によって、日本の企業は営業秘密漏えいのリスクを強く認識することとなった。

営業秘密侵害の危険性の高まりを受けて、2016 年 1 月に改正不正競争防止法が施行され、損害賠償請求における立証責任の軽減、実行行為者や背後の主犯たる法人に対する法定刑の引き上げ等、民事・刑事の両面での抑止力の向上が図られたが、その後もこの種の事件は頻発している。ここ数カ月の報道だけでも、表 1 の通り多数の営業秘密漏えい事案が発生しており、企業をとりまく状況は深刻さを増していることがうかがえる。

■表 1　営業秘密の漏えい事例

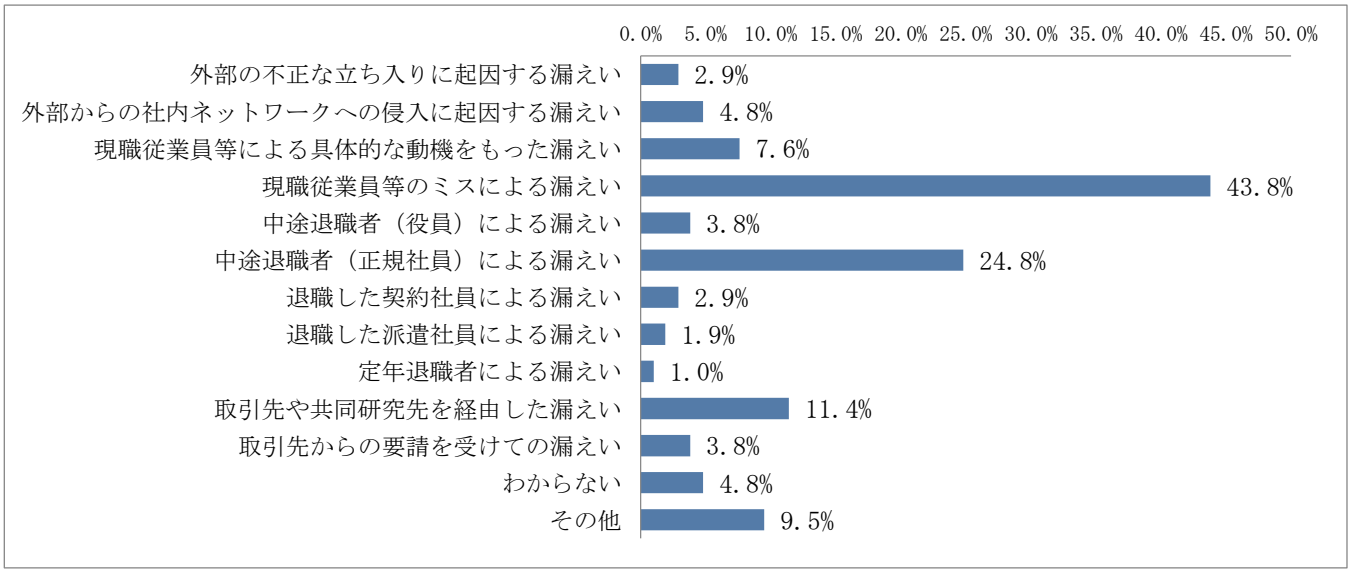
公表年月	企業	概要
2018 年 3 月	D 社	元役員が従業員名簿や提案書を不正に取得し競合他社へメールで送信。不正競争防止法で逮捕される。D 社は元役員と流出先企業に損害賠償を求め提訴。
2018 年 2 月	E 社	外部からの不正アクセスにより、顧客 2 万 8,700 人分の個人情報が流出。第三者が E 社の顧客情報を不正に取得した可能性があるという親会社からの連絡により発覚。警察・外部機関と連携し調査中。
2018 年 2 月	F 社	2 万 6,000 人分の顧客情報が漏えい。従業員がオンラインストレージに顧客情報をアップロードし漏えいさせた。F 社は従業員を刑事告訴する予定。
2017 年 10 月	G 社	退職後に使用する目的で従業員が図面データを複製。中国企業にデータを渡し 250 万円を受け取っていた。G 社は当該従業員を解雇し告訴。

出典：各種報道機関・公開情報をもとに弊社作成

独立行政法人情報処理推進機構（IPA）の調査[1]（以下、「IPA 調査」）によると、「過去 5 年間に営業秘密の漏えいがあった」と回答した企業が 8.6%存在する。特に従業員数規模 3,000 人超の企業においては、回答者全体の 2 割程度を占めており、いかなる企業も営業秘密漏えいリスクと無縁でないことがわかる。

図 1 は、IPA 調査において営業秘密の漏えいが発生した企業から得られた、漏えいのルートについての回答結果である。現職従業員、退職者、取引先、外部者等、さまざまなルートから漏えいが発生していることがわかる。なお、漏えいルート別の典型的な事例を表 2 にまとめた。

■図 1　営業秘密漏えいルート（n=105）



出典：IPA「企業における営業秘密管理に関する実態調査 -調査報告書-」

■表 2　漏えいルート別の情報漏えい事例

漏えいルート	典型的な事例
現職従業員からの漏えい	・　親切心から技術指導したことがきっかけで営業秘密が外部に漏えい ・　現職従業員が金銭的な目的で営業秘密を競合企業に提供
退職者からの漏えい	・　技術情報保有者の競合企業への転職に伴う技術情報の漏えい ・　営業部門担当者の競合企業への転職に伴う顧客情報・取引情報の漏えい
取引先等からの漏えいまたは不正使用	・　大口の取引先から「図面を見せてほしい」と言われ、断れず提示したところ競合企業に漏えい ・　取引先の管理不十分で相手方の従業員や再委託先を通じ営業秘密が漏えい
外部者からの漏えいや不正使用	・　外部者からのサイバー攻撃（標的型攻撃）により営業秘密が漏えい ・　外部からの訪問者に工場内部を無断で撮影され、工場の生産ラインのレイアウトに関する情報が競合企業に漏えい

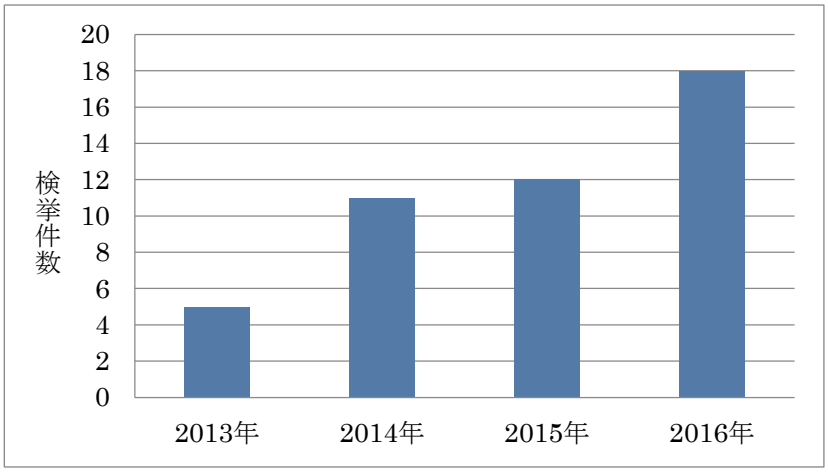
出典：IPA「企業における営業秘密管理に関する実態調査 -調査報告書-」、経済産業省「秘密情報の保護ハンドブック[2]」、過去の各種報道等をもとに弊社作成

[1] IPA が 2016 年 10 月～2017 年 1 月に行った「企業における営業秘密管理に関する実態調査」。無作為に抽出した 1 万 2,000 社にアンケート調査票を郵送し、2,175 社から回答を得ている。その結果は 2017 年 3 月 17 日に「調査報告書」として発表された。https://www.ipa.go.jp/files/000057774.pdf

[2] 経済産業省「秘密情報の保護ハンドブック」（2016 年 2 月）
http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf

図 2 は、警察庁が発表している営業秘密侵害事犯の検挙件数の推移である。営業秘密漏えいに関わる犯罪は年々増加傾向にある。

■図２　営業秘密侵害事犯の検挙件数



出典：警察庁「平成 28 年における生活経済事犯の検挙状況について[3]」をもとに弊社作成

（2）営業秘密漏えい事件多発の背景

営業秘密漏えいリスクの高まりの背景には、表 3 のような社会動向の急激な変化があると考えられる。このような社会動向は今後も続くであろうことから、営業秘密漏えいのリスクはますます高まっていく可能性は否定できない。

■表３　営業秘密漏えいリスクに関する社会動向の急激な変化

項目	解説
人材の流動化	日本の終身雇用の慣行が崩れつつある中、人材不足による労働力の奪い合いも相まって、同業他社への転職者が増えつつある。
情報端末の高度化	スマートフォンやタブレット等の小型で大容量の情報端末が急速に普及し、大量の情報が簡単に盗取等される危険性が増している。
データの利活用機会の増加	あらゆるデータがデジタル化された状態でストックされ、また有効に分析・活用されることで、情報自体が企業経営の貴重な財産（競争力の源泉）となっていることが多い。
サイバー攻撃の増加	多発・高度化する標的型攻撃等のサイバー攻撃により、営業秘密が漏えいする危険が増大している。

出典：IPA「企業における営業秘密管理に関する実態調査 -調査報告書-」をもとに弊社作成

[3] 警視庁ホームページ「平成 28 年における生活経済事犯の検挙状況等について」
http://www.npa.go.jp/publications/statistics/safetylife/kezai.html

（3）営業秘密漏えいのリスク

営業秘密漏えいによって被る企業の経済的損害については、表 4 を参照されたい。

■表 4　企業が被る経済的損害

No.	経済的損害	事例
1	競争力の低下による利益の喪失	営業秘密情報を失う、または競合他社に流出することにより、自社の競争力の低下を招く。
2	社会的信用の低下、取引先等との信頼関係の毀損による利益の喪失	顧客の個人情報や取引先等から開示を受け保有していた秘密情報等が漏えいした場合などにおいて、社会的信用低下や、取引先等との信頼関係の毀損を招く。
3	顧客や取引先等に与える損失の補てん、損害賠償等	営業情報等が流出したことにより、顧客や取引先等に与えた経済的な損失を補てんしなくてはならない可能性がある。この場合、相手方に対して支払う損害賠償金等の損害に加えて、顧客や取引先対応（含む訴訟対応）に伴う多額のコストを負担する場合がある。
4	加害者に対する責任追及に要するコスト	被害回復のために加害者に対する責任追及を行う場合は、弁護士費用や証拠保全のための費用等法的措置に要する一定のコスト負担が生じる。
5	原因調査や再発防止策に要するコスト	漏えいの拡大や再発の防止のためには、徹底した原因調査と再発防止策の実施が欠かせない。

出典：経済産業省「秘密情報の保護ハンドブック」、IPA「企業における営業秘密管理に関する実態調査 –調査報告書–」をもとに弊社作成

損害額の多寡は漏えいした情報の質・量によるところが大きいため、一概に論じることはできないが、コア事業の競争力を支えるような情報が競合他社に流出した場合等における当該企業の被る経済的な損失は、甚大なものとなることは容易に想像できる[4]。

逆に、他社との共同研究、転職者の受け入れ、取引の中での秘密情報の授受等の際に、意図せず他社の営業秘密を侵害する場合があることにも注意する必要がある。紛争に巻き込まれれば、訴訟対応費用を含めた賠償損害[5]はもちろん、事件報道等による社会的な信用への影響も避けられない。

[4] 2012 年鉄鋼メーカーの事例では 1,000 億円の損害賠償請求訴訟が、2014 年電機メーカーの事例では約 1,100 億円の損害賠償請求訴訟が提起されている。

[5] 他社からの営業秘密の開示が不正な開示であることを知らなかったとしても、知らないことにつき「重大な過失」があるとされるときには、不正競争防止法上、その営業秘密の使用や別の他社への開示行為が損害賠償請求や差止請求の対象となる。

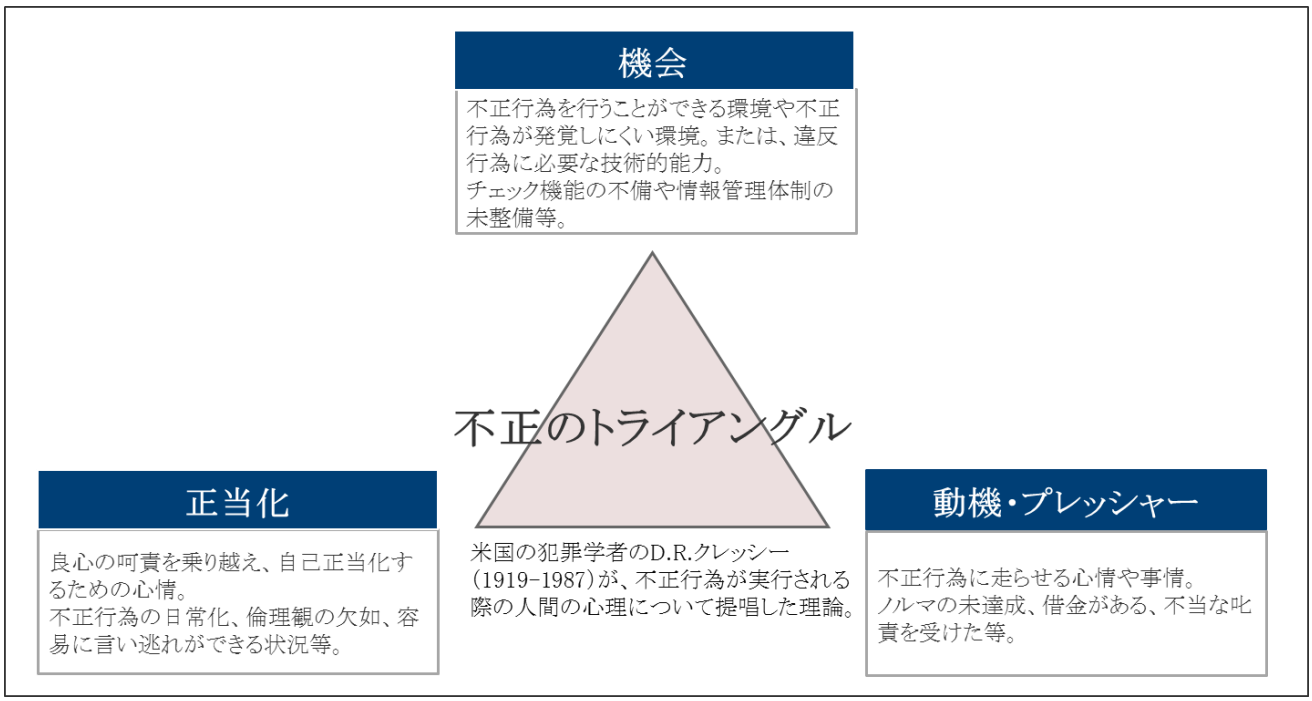
2．営業秘密漏えい防止策

前章で述べたように、営業秘密の漏えいリスクは高まっており、企業は営業秘密の漏えい防止対策を強化すべきである。具体的な漏えい防止対策については、経済産業省「秘密情報の保護ハンドブック」に、「従業員等」「退職者等」「取引先」「外部者」への対策が対象ごとに詳しく解説されているため、同ハンドブックを参照することをお勧めする。

ここで本章では、従業員や退職者といった内部関係者の不正対策に焦点を当て、その対策案の検討にあたって、企業が持つべき視点について述べる。

米国の犯罪学者 D.R.クレッシー（Donald Ray Cressey）が提唱した「不正のトライアングル」という理論がある。この理論では、不正を行う「機会」、不正行為は仕方のないものであるとする「自己正当化の心理」、問題を抱える者が不正を犯してでも問題を解決したいという「動機・プレッシャー」の 3 つの要因が揃ったときに人間は不正行為を行いやすいとしている。内部不正防止の対策において、企業はこの 3 つの要因を不正行為の実行者から奪うことが重要なのである。

■図３　不正のトライアングル



出典：弊社作成

経済産業省「秘密情報の保護ハンドブック」においても、やみくもに対策を実施するのでなく、5 つの「対策の目的」に沿った形で具体策を検討すべきとしている。この 5 つの「対策の目的」が、「機会」「正当化」「動機・プレッシャー」の封じ込めを意味していると考えると理解しやすい。

表 5 にそれぞれの関連を整理し、代表的な対策の具体例を示す。

■表５　営業秘密漏えい内部不正防止対策

No.	対策の目的 （「秘密情報の保護ハンドブック」参照）	封じ込める 不正の要因	具体例
1	秘密情報に近寄りにくくする	機会	・　秘密情報にアクセスできる人を最小限に止める。 ・　退職者に対しては速やかにアクセス権を削除する。
2	秘密情報の持ち出しを困難にする		・　私物 USB メモリの社内使用を禁止する。 ・　電子データを暗号化する。 ・　秘密情報が記された会議資料等を適切に回収する。 ・　社外へのメール送信を制限する。
3	漏えいが見つかりやすい環境をつくる		・　防犯カメラを設置する。 ・　情報システムのログをチェックする。 ・　入退室を記録する。 ・　名札着用を徹底する。 ・　内部通報窓口を設置する。
4	不正行為者に「秘密情報だと思わなかった」という言い逃れを許さない	正当化	・　秘密情報の取り扱い方法に対するルールを周知する。 ・　秘密保持契約等を締結する。 ・　秘密情報である旨の表示（マル秘表示）を行う。
5	社員のやる気を高め、秘密情報を持ち出そうという考えを起こさせない（企業への帰属意識の醸成、仕事へのモチベーションの向上）	動機・ プレッシャー	・　長時間労働の抑制、福利厚生の充実、良好な職場コミュニケーション等により、働きやすい職場環境を整備する。 ・　透明性が高く公平な人事評価を行う。

出典：経済産業省「秘密情報の保護ハンドブック」をもとに弊社作成

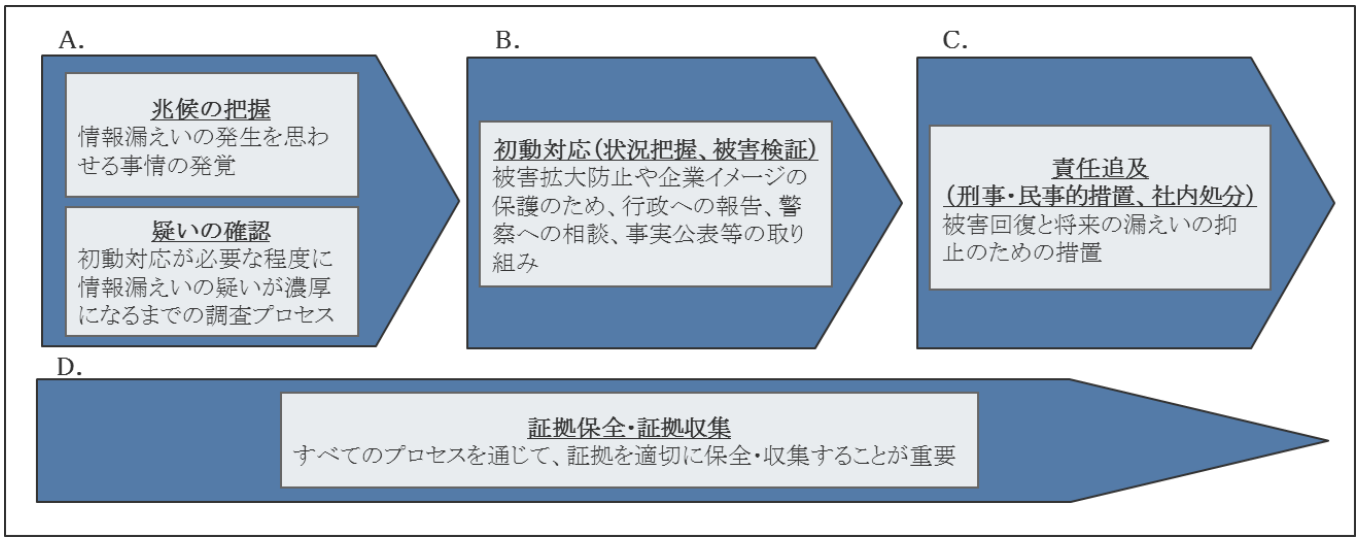
３．営業秘密漏えい発覚時の対応

企業が十分な対策を講じたとしても、営業秘密の漏えいを完全に防ぐことは難しい[6]。営業秘密の漏えいが発覚した際、更なる情報の漏えい（拡大）を防ぎ、企業の被る損害を最小限に食い止め、また企業の信頼回復を早期に実現するためにも、事件発生後の対応が肝要である。以下に、営業秘密が漏えいした際の企業のとるべき対応を述べる。

一般的に営業秘密の漏えいが発生した、またはそのおそれがある場合の基本的な対応の流れは図 4 の通りである。

■図４　営業秘密漏えい時の一般的な対応フロー

A.　兆候の把握・疑いの確認：情報漏えいの兆候を確認し、初動対応の必要性を検討
B.　初動対応（状況把握、被害検証）：被害拡大防止や企業イメージの保護のための取り組み
C.　責任追及（刑事・民事的措置、社内処分）：被害回復と将来の漏えいの抑止のための措置
D.　証拠保全・証拠収集：上記すべてのプロセスと同時並行に行う、証拠の適切な保全・収集



出典：経済産業省「秘密情報の保護ハンドブック」をもとに弊社作成

企業においては、有事に備えて上記の対応の流れを理解しておく必要があるが、特に認識しておくべきポイントは以下の 3 点である。

（1）事実調査（A. 兆候の把握・疑いの確認、 D. 証拠保全・証拠収集）

営業秘密が漏えいした兆候や疑いが生じた場合は、一刻も早く事実調査（調査および証拠の保全・収集）を行う必要がある。事実調査が不十分または不適切な場合は、その後の対応に支障をきたす可能性があるため、事前に大まかな対応要領を定めておくことが望ましい。

特に注意すべきは内部犯への対応である。内部犯は自らが疑われていると気が付くと、私的に保存した情報やデータの消去・破棄等により証拠隠滅を図るおそれがある。そのため内部犯による情報漏えいのおそれがある場合は、調査は限られた一部の人間によって秘密裏に行う必要がある。また、内部の容疑者にヒアリングを実施する際、一度ヒアリングを行ってしまうと、容疑者は二度と出社して

[6] 例えば、対策を講じる前に退職した者がすでに持ち出した情報について、企業はコントロールできない。

こなくなるケースがあるため、実施の方法・場所・手順等を慎重に検討し、段取りよく行う必要がある。

（2）対外対応（B. 初動対応）

事実調査を実施し情報漏えいの事実を確認すると、社外の関係先への報告・謝罪および状況次第ではマスコミ対応等による情報の公表が求められる。

顧客や取引先の情報が漏えいした場合は、顧客・取引先の二次被害防止の観点から、一刻も早く漏えいした事実の報告や注意喚起を行うべきである。その後に事実関係が判明次第、都度追加の報告を行う等、誠心誠意の対応が求められることは言うまでもない。

また社会全般に及ぼす影響が大きい場合、世間一般へ事件の公表を行う必要がある。事件・事故の重大性に応じてホームページでの公表・記者会見・取材対応等の中から適切な公表方法を選択することになる。

なお、漏えいした情報の内容や重要度によっては、監督官庁や株主・証券取引所への報告が必要となるケースもあるので注意が必要である。

■表６　対外対応

No.	関係先（例）	概要
1	顧客・取引先	顧客・取引先の情報が漏えいした場合は、迅速に謝罪・報告し、その後も適宜調査結果が判明次第、報告を継続する。
2	世間一般	事件の重大性を考慮して、公表の是非および公表方法（ホームページ、記者会見、取材対応等）を検討する。
3	警察	不正競争防止法違反を根拠に被害届を提出することを検討する。個人のパソコンの操作履歴等、詳細な調査を行うためには警察の協力が必要な場合がある。
4	監督官庁	特に個人情報が漏えいした場合には、個人情報保護法に基づいて報告を行う。
5	株主、証券取引所	証券取引所では事実関係開示のルールが定められている。

出典：弊社作成

（3）不正競争防止法による救済（C. 責任追及）

対外への対応に一定の目処が立った後は、被害の回復のための措置を取ることが必要であるが、不正行為の被害により情報が漏えいした場合は、不正競争防止法による救済措置がある[7]。

被害を受けた企業には差止請求権があり、不正競争防止法に違反する不正競争行為によって営業上の利益を侵害される、またはそのおそれがある場合に、営業秘密の侵害行為の停止の請求や将来の侵害行為の予防の請求、侵害行為のために使用された記録媒体等の廃棄の請求を行うことができる。また、損害賠償の請求や、（営業上の利益が侵害された場合には）不当利得の返還請求、（営業上の信用を害された場合には）謝罪広告等の信用回復のための措置の請求、刑事責任の追及といった権利もあ

[7] 経済産業省「不正競争防止法違反被害への救済」
http://www.meti.go.jp/policy/ipr/infringe/remedy/remedy03-5.html

る。

ただし、不正競争防止法では、営業秘密に該当するための一定の条件が定められている。営業秘密が 1. 秘密として管理されていること（秘密管理性）、2. 有用な営業上または技術上の情報であること（有用性）、3. 公然と知られていないこと（非公知性）の 3 要件をすべて満たすことである。表 7 にそれぞれの要件の概要と具体的な例を示した。なお、この 3 要件は、「知的所有権の貿易関連の側面に関する協定（TRIPS 協定）[8]」で定められている保護水準を満たしており、この要件をクリアすると日本国内のみならず世界的な保護水準も満たすことになる。

企業において、不正競争防止法による法的な保護を受けるためには、営業秘密の 3 要件を満たすための措置を講じておくことが重要である。

■表７　営業秘密の３要件の概要

No	営業秘密の要件	概要	具体例 （〇あてはまる、×あてはまらない）
1	秘密管理性	情報へアクセスできる者を特定し、アクセスした人が「当該情報は秘密である」と認識できる状態にあるもの。	〇 会社にとって秘密にしたい情報であるとアクセスした人がわかる程度に、紙や電子記録媒体への「マル秘」表示がされた情報 〇 管理責任者が設置された情報や管理方法がルール化された情報 ※上記はあくまで一例であり、企業の実態や規模等に応じた合理的な手段でよいとされる。
2	有用性	客観的にみて営業上または技術上有用な情報であること。 事業活動に使用されるものや費用、経営効率の改善等に役立つもの。	〇 「ある方法に取り組んだが役に立たない」という失敗の知識や情報 × 脱税情報や有害物質の垂れ流し情報等、公序良俗に反する内容の情報
3	非公知性	情報の保有者の管理下以外では一般に入手できないもの。 公知情報の組み合わせであっても、その容易性やコストによっては非公知性が認められ得る。	〇 当該情報を知っているものに守秘義務が課せられている情報 × ホームページや書籍、学会発表等から容易に引き出すことができると証明できる情報

出典：経済産業省資料[9]をもとに弊社作成

[8]「知的所有権の貿易関連の側面に関する協定（Agreement on Trade-Related Aspects of Intellectual Property Rights；TRIPS 協定）」とは、1995 年に WTO が設立された際の主要な付属協定書の一つで、知的財産権全般（著作権および関連する権利、商標、知的表示、意匠、特許、集積回路配置、非開示情報）を保護する国際協定である。

[9] 経済産業省「産業構造審議委員会知的財産政策部会 技術情報の保護等の在り方に関する小委員会 営業秘密の管理に関するワーキンググループ」配布資料　http://www.meti.go.jp/committee/materials2/downloadfiles/g91225a06j.pdf

4．おわりに

本稿では、営業秘密漏えいリスクに関し、近年の実態、企業の被る損害、そして企業がとるべき対策・対応について述べた。営業秘密漏えい事件は多発しており、昨今の社会動向を踏まえると、今後も情報漏えいリスクが高まる可能性は否定できない。営業秘密漏えいが発生すると、内容次第では企業の経営に大きな影響を及ぼすリスクがあることから、企業においては「内部犯による意図的な侵害行為」を念頭に置いた防止対策を多面的に講じておくことが有効である。また、万が一事件が発生した際は、被害を最小限に食い止め早期に信頼を回復するための事後対応が重要である。

有事の対応力向上のために、事前に検討できる対応を予め準備しておくことが有効である。

［2018 年 4 月 20 日発行］

東京海上日動リスクコンサルティング株式会社

経営企画部 兼 ビジネスリスク本部　研究員　三保 春彦 （専門分野：リスクマネジメント）
〒100-0004 東京都千代田区大手町 1-5-1 大手町ファーストスクエア ウエストタワー23 階
Tel. 03-5288-6712　Fax. 03-5288-6625
http://www.tokiorisk.co.jp/