

# 「営業秘密管理指針」の活用

東京グラフィックス専務理事 齋藤 成

情報のデジタル化やIT化社会の進展に伴い、企業の情報漏洩のトラブルが増えています。これは管理体制の不備による個人情報や営業秘密の流出、また、インターネットを介しての社員による不適切な発言やファーストフード店での映像などが問題になっており、企業が受けるダメージは大きなものとなってきました。内部統制<sup>\*1</sup>ということになりますが、当業界でも自社開発商品の模倣、退職者の転職による営業秘密の流用や顧客情報の管理が問題になることもあります。

知的財産の保護については、著作権法改正による海外の海賊版対策への対応や電子書籍への“電子出版権”の創設がされようとしています。一方、機密漏洩の防止については、不正競争防止法の改正(平成23年12月)により営業秘密侵害罪の適用、そして営業秘密管理に対する指針(経済産業省発行)も整ってきました。

企業内機密情報の中には個人情報がありますが、その保護については、会員企業の約100社がプライバシーマークを付与され、個人情報保護への意識と実際の活動は顕著に向上しています。印刷・関連業の場合、これまでも個人情報に限らず顧客や自社の機密情報の保護には格段の注意が払われてきました。ここでは、改正不正競争防止法<sup>\*2</sup>に伴う経済産業省が公表している「営業秘密管理指針」(平成25年8月16日改訂)から、個々の企業が営業秘密を守る観点で情報漏洩を防止することの徹底を図っていきたいと考えています。

ここで示されている営業秘密管理については、個人情報保護の手法と非常に似たもので、プライバシーマーク制度(あるいは情報セキュリティーマネジメントシステム: ISMS、ISO27001: 2005)と軌を一にした管理方法です。プライバシーマークを付与されていない事業者にとっても有用な方法であり、プライバシーマークを付与されている事業者にとっては個人情報保護を営業秘密管理に置き換えれば同等の管理方法で対応できます。「東京グラフィックス」誌では、3回に分けてこの営業秘密管理について連載します。是非参考にしてください。

- \* 1 : 内部統制における法令としては、個人情報保護法、不正競争防止法、公益通報者保護法などがあります。
- \* 2 : 不正競争防止法の対象は、「営業秘密」です。企業の「個人情報」は営業秘密情報として管理しておかなければ不正取得、漏洩を不正競争防止法に問えません。

## ■中小企業における対策

各種情報が漏洩した場合、顧客からの信用が低下するだけでなく、新たな顧客獲得の機会も失うことになります。また、顧客から損害賠償訴訟を起こされてしまうこともあります。

このような事態にならないためにも、企業として情報漏洩防止対策を講じることが重要となりますが、対策が後回しになるケースが多く見受けられます。対策が遅れる要因としては、人材や予算に限りがある、具体的にどのような対策をしてよいか分からない、自社のセキュリティ対策方針が明確になっていない、などが挙げられます。とはいえ、機密情報を守る方策を立てないでいることは危険極まりない状態です。

そこで自社にとって大事な情報を大切に保護することから始まります。企業価値の源泉は他社との差別化にあり、企業は自らの強みを明確に意識してそれが他社に真似されないように自衛策を講じる必要があります。次に自社の従業員が他社の営業秘密を侵害しないこと。そして企業と従業員が共通の意識をもって取り組む。つまりヒトの要素に着目することが重要です。

企業は『侵害されないための防衛策』、『侵害しないための予防策』の両面から適切な管理が求められます。

## ■営業秘密の保護

情報漏洩で問題となるものには、顧客などの個人情報のほかに、会社の事業に関する営業秘密があります。

営業秘密とは、設計図、製法・製造ノウハウ、販売マニュアル、仕入先リストなどを指します。印刷会社であれば印刷

物に含まれる公開前の各種データや著者による未発表論文、各種名簿、名刺、発送リストといった顧客に所有権があるもの等、制作過程で守秘義務を負うもの。また、個人情報も営業秘密の一つとされています。特に、知的財産に該当するような独自の製法・製造ノウハウは、特許取得などで積極的に権利化できるものもあるため、その管理の重要性は高くなります。

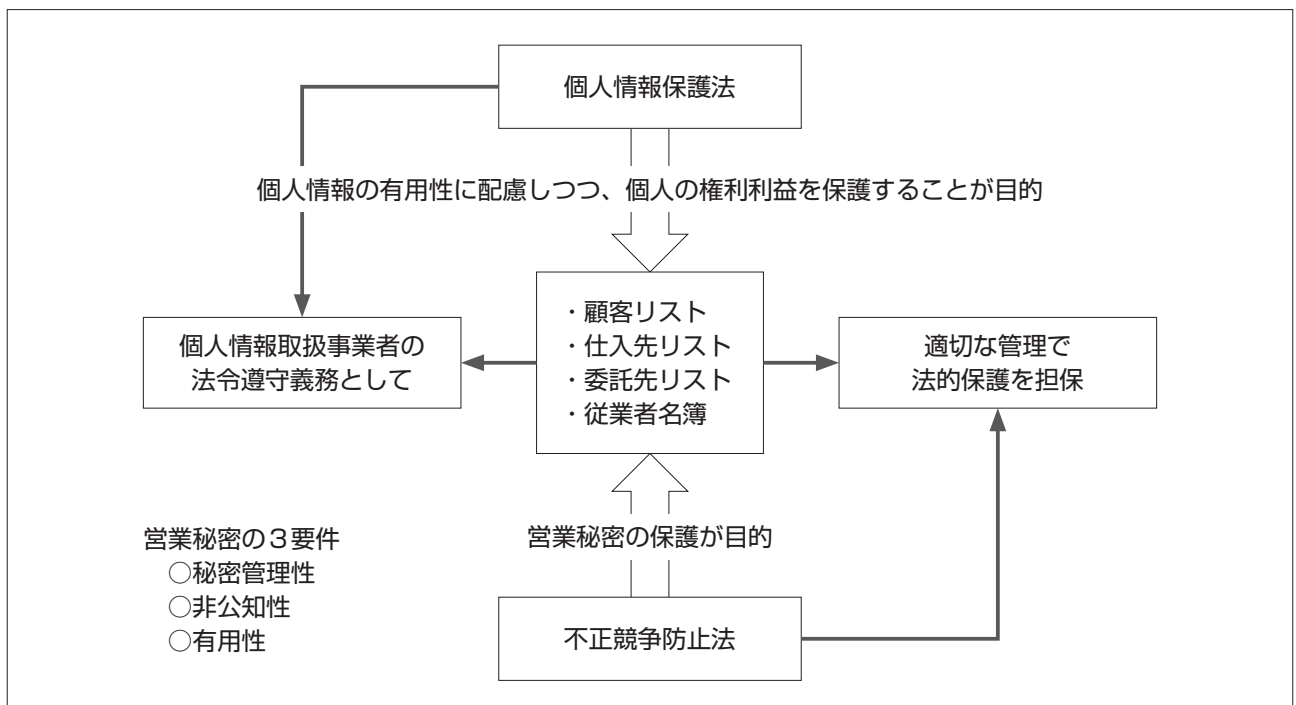
これらの営業秘密は、不正競争防止法で保護されます。営業の秘密として保護されるためには、①秘密として管理されている（秘密管理性）、②有用な営業上または技術上の情報（有用性）、③公然と知られていない。保有者の管理下以外では一般に入手できない（非公知性）、の3要件をすべて満たす必要があります。次回から具体的にみていきましょう。

※経済産業省「営業秘密管理指針」URL

<http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/111216hontai.pdf>



個人情報保護と不正競争防止法の関係



### ●営業秘密として不正競争防止法で保護される3要件

〔秘密管理性〕（秘密として管理されていること）

従業員や外部者等が管理状況を見た際、秘密として管理していると認識できる状態にあること。

- ①情報にアクセスできる者を制限していること（アクセス制限）
- ②情報にアクセスした者がそれが秘密であると認識できること（客観的認識可能性）

〔有用性〕（有用な情報であること）

事業活動に使用されていたり、使用されることによって、経費の節約、経営効率の改善等に役立つものであること。

〔非公知性〕（公然と知られていないこと）

情報の保有者の管理下以外では一般に入手できないこと。

### 【参考】不正競争防止法（抜粋）

第二条 この法律において「不正競争」とは、次に掲げるものをいう。

※一～三、十～十五略

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。）

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、又は開示する行為

※第二条2～5、7～10略

6 この法律において「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をいう。

（差止請求権）

第三条 不正競争によって営業上の利益を侵害され、又は侵害されるおそれがある者は、前項の規定による請求をするに際し、侵害の行為を組成した物（侵害の行為により生じた物を含む。第五条第一項において同じ。）の廃棄、侵害の行為に供した設備の除却その他の侵害の停止又は予防に必要な行為を請求することができる。

（損害賠償）

第四条 故意又は過失により不正競争を行って他人の営業上の利益を侵害した者は、これによって生じた損害を賠償する責めに任ずる。ただし、第十五条の規定により同条に規定する権利が消滅した後にその営業秘密を使用する行為によって生じた損害については、この限りでない。

## クラウドサービス利用の注意点

最近、多くの企業でクラウドサービスの利用が進んでいます。印刷会社でもコスト軽減やデータ保管を中心に活用されていますが、先ごろ大手サーバ会社による大量のデータ消失事故も起こりました。そこで、今一度クラウドサービスについて注意点を記しました。併せて、クラウドの利用については行政（総務省、IPA等）でもWeb上でパンフレットが用意されていますので参考にしてください。

クラウドサービスはインターネット経由で提供されるため、ネットワークに障害が出ると、完全に使えなくなります。また、情報やセキュリティの管理を業者に一任することになるため、業者に対する信頼性が重要です。情報漏洩や消失時に対応できないため、莫大な損失が出る可能性を捨てきれません。さらに、開発や一般に対するコンテンツ提供の仕方を業者の提供するサービスに合わせる必要があるため、自由に開発や提供ができるわけではないという問題があります。

クラウドサービス上のデータは、クラウドサービス事業者により安全に管理されることが基本ですが、実際には障害によるデータ消失や情報漏洩などの事故も発生してい

ます。ですから利用するにあたっては、想定される脅威への対策が必要です。主な脅威として、以下の3点を挙げておきます。

### ①障害によるデータ消失

クラウドサービスに障害が発生した場合、クラウドサービス上だけにデータを預けているとデータの復旧ができなくなる恐れがあります。クラウドサービスを利用する際には別のシステムで定期的なバックアップを取っておきましょう。

### ②データの外部漏洩

クラウドサービス事業者へのサイバー攻撃等で預けているデータが外部に漏洩する可能性があります。契約するクラウドサービス事業者のセキュリティ対策のレベルや保証の範囲等をよく確認しましょう。

### ③クラウドサービスのアカウントの第三者による悪用

ウイルス感染等によって、利用しているクラウドサービスのユーザIDやパスワードが流失した場合、第三者による不正アクセスにより情報が漏洩する可能性があります。そこでユーザIDやパスワードは個別のサービス毎に異なるものを設定し使い回しをしないようにしましょう。

## 【参考】中小企業のためのクラウドサービス安全利用チェックシート

チェック	項目	内容
<b>【A】クラウドサービスの利用範囲についての確認項目</b>		
<input type="checkbox"/>	利用範囲の明確化	クラウドサービスでどの業務、どの情報を扱うかを検討し、業務の切り分けや運用ルールの設定を行いましたか？
<input type="checkbox"/>	サービスの種類とコスト	業務に合うクラウドサービスを選定し、コストについて確認しましたか？
<input type="checkbox"/>	扱う情報の重要度	クラウドサービスで取扱う情報の管理レベルについて確認しましたか？
<input type="checkbox"/>	ポリシーやルールとの整合性	セキュリティ上のルールとクラウドサービスの活用の間に矛盾や不一致が生じませんか？
<b>【B】クラウドサービスの利用準備についての確認項目</b>		
<input type="checkbox"/>	担当者	クラウドサービスの特徴を理解した担当者を社内に確保しましたか？
<input type="checkbox"/>	ユーザ管理	クラウドサービスのユーザについて適切に管理できますか？
<input type="checkbox"/>	パスワード	パスワードの適切な設定・管理は実施できますか？
<input type="checkbox"/>	データの複製	サービス停止等に備えて、重要情報を手元に確保して必要なときに使えるための備えはありますか？
<b>【C】クラウドサービス提供条件等についての確認</b>		
<input type="checkbox"/>	事業者の信頼性	クラウドサービスを提供する事業者は信頼できる事業者ですか？
<input type="checkbox"/>	サービスの信頼性	サービスの稼働率、障害発生頻度、障害時の回復目標時間などのサービスレベルは示されていますか？
<input type="checkbox"/>	セキュリティ対策	クラウドサービスにおけるセキュリティ対策が具体的に公開されていますか？
<input type="checkbox"/>	利用者サポート	サービスの使い方がわからないときの支援（ヘルプデスクやFAQ）は提供されていますか？
<input type="checkbox"/>	利用終了時のデータの確保	サービスの利用が終了したときの、データの取扱い条件について確認しましょう。
<input type="checkbox"/>	契約条件の確認	一般的契約条件の各項目について確認しましょう。

※ IPA「中小企業のためのクラウドサービス安全利用の手引き」から