「営業秘密管理指針」の活用

東京グラフィックス専務理事 斎藤 成

6－7年前になりますが、プライバシーマークが今ほど普及していない頃です。プライバシーマークを申請されたA社に審査に出向いたところ、そこでは個人情報は従業員情報程度しか保有されていませんでした。何故、プライバシーマークを必要とされるか代表者に伺った際に、「当社には個人情報はなきに等しい状態です。しかし、顧客からお預かりしている情報はまさに機密情報ばかりです。そこで、プライバシーマークと同様の管理方法でそうした顧客の重要な情報を取扱うことで、顧客への信頼と自社の管理体制が確立できればよいと考え、Pマーク物件とシークレットの“Sマーク物件”に区分し、管理しようとしております。機密情報の取扱いこそ、当社の根幹に関わっておりますから」とのお答えに、納得したものです。ここで紹介している営業の秘密管理は、A社の代表者が示された“Sマーク”の発想と同様だと考えられます。

「営業秘密管理」を具体的にどのように管理していけばよいでしょうか。これも『個人情報保護』と似た管理方法でよいと考えます。それでは、具体的にみていきましょう。

■組織的管理方法

物理的管理、技術的管理、人的管理（秘密保持契約）

営業秘密を保護する管理のあり方ですが、営業秘密の管理はどのような保護、成果を求めるかによってそれに必要な管理の水準は異なります。

管理の対象（情報･ヒト）の明確化により、過大なコストを避けつつ、実効的な管理を行うことが可能となります（少なくとも過去の裁判例で保護の要件のレベルの管理は必要です）。

裁判の判例にみる秘密管理性とは、アクセス制限を例にとると、アクセスした人が、管理の対象となっている情報を秘密と認識し、またアクセス権限のある人がそれを秘密として管理することに関する意識を持ち、責務を果たす状況になっていることです。

具体的には、アクセスできる人が限定され、権限のない者によるアクセスを防ぐ手段が取られている。①管理者の人数の限定、②施錠されている保管室への保管、③事務所内への外部者の入室の禁止、④電子データの複製の制限、⑤コンピュータへの外部者のアクセスの防止措置、⑥システムの外部ネットワークからの遮断、⑦㊙等の印の押印、⑧従業員が秘密管理の責務を認知するための教育の実施、⑨就業規則における秘密保持義務の明確な規定、⑩誓約書や秘密保持契約による責務の設定。

上記が機能するように組織として仕組みを持つこと。つまり、情報の扱いに関する上位者の判断を求めるシステムの存在と、外部アクセスに関する応答に関する手順の設定が求められます。

【物理的管理】

①情報の区分と表示
- 秘密情報は、その他の情報と区分して管理する。
- 情報については、秘密性のレベル（例.「厳秘」「秘」「取扱注意」等）を決め、レベルに応じた管理を行う。
- ㊙マーク等を付す。
- 他社の営業秘密が混入しないように出所を明示する。

②アクセス権者の限定
- 誰がどの営業秘密にアクセスできるかを予め特定する。
- 営業秘密へのアクセス記録を残す。

③媒体の保管、持ち出しと廃棄
- 営業秘密を記録した媒体は、施錠可能な保管庫に施錠した上で保管する。
- 営業秘密を記録した媒体の持ち出しを制限する。
- 営業秘密を記録した媒体を廃棄する際には、焼却やシュレッダーによる処理、溶解、破壊等の措置を講じる。

④施設等の管理
- 営業秘密を記録した媒体が保管されている場所を施錠する。
- 営業秘密を記録した媒体が保管されている施設への入退室を制限する。

【技術的管理】

①マニュアル等の設定

・事前に電磁的に記録されている営業秘密の管理方法やデータ複製、バックアップを行う際のルールをマニュアル化・システム化する。

②アクセス及び管理権者の限定

・コンピュータやファイルそのものの閲覧に関するＩＤやパスワードを設定する。

・アクセス記録をモニタリングする。

・情報セキュリティの管理者が退職した際には、管理者パスワードを確実に変更する。

③外部からの侵入に対する防御

・営業秘密を管理しているコンピュータを何らかの形で外部ネットワークから遮断する(インターネットに接続しない、ファイアーウォールの設置等)。

・ウイルス対策ソフトウェアを導入する。

・ファイル交換ソフトウェアや不必要なソフトウェアをインストールしない。

④データの消去、廃棄

・秘密情報を使用・保管していたコンピュータ・サーバ等の機器類を廃棄、譲渡する場合にデータ復元ができない方法により記録を消去する。

・上記の場合に、コンピュータ機器等を物理的に破壊する。

【人的管理】

①教育・研修の実施

組織体制内に教育・研修責任者を設置し、秘密管理の重要性や管理組織の概要、具体的な秘密管理ルールについて、日常的に教育・研修を実施すること。

②役員・従業員

就業規則や各種規程に秘密保持義務を規定し、在職中の役員・従業員が負う秘密保持義務を明らかにする。

③退職者

退職者に秘密保持義務を課す場合には、対象を明確にした秘密保持契約を締結することが必要である。

※退職者に競業避止義務を課す場合は、競業制限の期間や場所的範囲、制限する業種の範囲が合理的範囲内でないと有効性が認められない点に注意。

④派遣従業者

派遣従事者に対して秘密保持義務を課す場合には、雇用主である派遣元事業者との間で秘密保持契約を締結し、派遣元事業者が派遣先に対し、派遣従事者による秘密保持に関する責任を負うこととする。

⑤転入者

他の会社からの転職者を採用する場合、他社の情報に関するトラブルを回避する観点から、転職者が前職で負っていた秘密保持義務や競業避止義務の内容を確認、また採用後も業務内容を定期的に確認すること。

⑤取引先

「営業秘密」を取引先に開示する場合、「秘密管理性」を維持するためには、秘密保持義務を含んだ契約を締結する必要がある。

■社員との守秘義務契約

現役の従業員については、就業規則で秘密保持義務が定められていることが多いですが、仮に就業規則で特段の規定がなくとも信義則上、秘密保持義務が認められるのが通例です。

これに対して、明示の特約がない場合の退職者の守秘義務違反は、「著しい信義則違反」があった場合に限定して認められており、特約がない場合の退職者の守秘義務の範囲は非常に限定的です。従って、就業規則や守秘義務契約により、予め明示的に秘密保持義務を課しておくことが必要です。退職者の守秘義務を確実なものとする上では、単に就業規則に定めておくだけでなく、退職前に従業員に秘密保持の誓約書を提出させることが望ましいでしょう。誓約書を提出させる時期としては、①入社時（誓約書の取得は容易であるが、保持すべき営業秘密の内容を特定できないため法的な効力は弱い)、②機密性の高いプロジェクトに参加させる時点など在職中（手間はかかるが、秘密保持の対象となる情報が容易に特定でき、かつ従業員に秘密保持への強い意識を持たせられるので最も効果的)、③退職時（秘密保持の対象となる情報の特定は容易であるが、突然に誓約書を要求しても退職する従業員の同意を得られない可能性がある)の3つが考えられます。

実務上は、入社時とプロジェクト等への参加時や退職時の両方で誓約書を提出させるなど、複数回誓約書を提出させることも一般的に行われています。

さて秘密保持契約を結ぶ際の内容を列記します。

対象となる範囲ですが、対象となる情報の範囲を特定することで当事者双方の認識を共通化し、実効的な秘密管理が

【参考】退職時の秘密保持誓約書の例（経済産業省資料から）

秘密保持誓約書

私は平成　　年　　月　　日付けにて、一身上の都合により、貴社を退社いたしますが、貴社の営業秘密に関して、下記の事項を遵守することを誓約します。

記

第1条　（秘密保持の確認）

私は、貴社を退職するに当たり、次に示される貴社の営業秘密に関する資料一切について、原本はもちろん、そのコピー及び関係資料等を貴社に返還し、自ら保有しないことを確認します。（＊1）

①製品開発に関する技術資料、製造原価及び販売における価格決定等の貴社製品に関する情報

②以下略

第2条　（退職後の秘密保持の誓約）

前条各号の営業秘密を、貴社退職後においても、不正に開示又は不正に使用しないことを約束します。

第3条　（契約の期間）

本契約は、○年間有効とします。ただし、第1条各号の営業秘密が公知となった場合は、その時点をもって本契約は終了することとします。（＊2）

第4条　（競業避止義務の確認）

貴社を退職するに当たり、退職後1年間、貴社からの許諾がない限り、次の行為をしないことを誓約します。

①貴社で従事した○○の開発に係る職務を通じて得た経験や知見が貴社にとって重要な企業秘密ないしノウハウであることを鑑み、当該開発及びそれに類する職務を貴社の競合他社において行いません。

②貴社で従事した○○に係る開発及びこれに類する職務を貴社の競合他社から契約の形態を問わず、受注ないし請け負うことをいたしません。

③貴社の顧客に関する重要情報も開示はいたしません。

④以下略

以上

平成　　年　　月　　日

株式会社　　△△印刷

代表取締役　○○○○殿

住　所＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

氏　名＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿（印）

＊1　秘密保持の対象とする情報の定義と呼称（例えば「営業の秘密」、「機密事項」など）については様々なものがあり、各事業者の就業規則その他の文書との整合性や営業秘密を保護する主旨を明確化することが望ましい。

＊2　契約の期間に関して、秘密保持義務についても、可能な限り期限を設定することが望ましいが、それが困難な場合は、営業秘密性が失われるまで存続する旨を明記することが望ましい。

可能となります。・メタ形式（概念）による特定　・媒体による特定　・詳細な（クレーム類似の）特定を範囲とする。次に、秘密保持義務と付随義務では、基本的義務として営業秘密の目的外使用の禁止　・アクセス権限のない第三者への開示禁止　・記録媒体の複製の禁止　・退職時の返還の明記。例外規定としては、開示前からすでに公知であった情報、開示後に受領者の責めに帰すべき事由なく公知となった情報、第三者から守秘義務を課されることなく取得した情報については例外とするのが望ましいでしょう。

STOP! “個人情報漏えい” 豆知識　IPA（情報処理推進機構）の資料から

■個人情報が書かれた書類を
シュレッダーなどにかけて廃棄していますか？

個人情報が書かれた書類をそのままごみ箱に捨てるようなことはしていませんか。ごみとして捨てられた書類から、個人情報が漏えいしてしまう危険性があります。必ず、シュレッダーにかけて、個人情報、業務情報が読み取れない状態で廃棄するようにしましょう。また、大量の書類を廃棄する必要があるときは、専門の業者に依頼するなどして確実に情報漏えいを防ぐようにしましょう。

また、PCを廃棄するときは、ハードディスクに記録されていた情報を完全に消去する必要があります。初期化をしただけでは、復元ソフトを使うことで読み取られてしまいます。データ消去ソフトを使用するか、ハードディスクを物理的に破壊してから廃棄するようにしましょう。

■ソフトウェアの脆弱性情報を把握し
必要に応じてパッチの適用を行っていますか？

OSやミドルウェアなどのソフトウェアには日々、セキュリティ上の弱点（脆弱性）が発見され、修正されています。ソフトウェアのパッチ更新を行っていない場合、弱点が長期間残ってしまい、セキュリティを確保できません。ソフトウェアの脆弱性情報を定期的に確認し、必要に応じてパッチを適用するなど、対策を行ってください。

◎JVN iPedia（脆弱性対策情報データベース）
http://jvndb.jvn.jp/
◎脆弱性対策情報収集ツール「MyJVN」
http://jvndb.jvn.jp/apis/myjvn/

■ファイアウォールを使用して
ネットワークを目的毎に分割していますか？

会社が使用するネットワークには、社内用や公開用など様々なものがあり、求められるセキュリティレベルも異なります。ファイアウォールを使用してこれらのネットワークを分割し、それぞれのネットワーク間で不要な情報がやり取りされないよう、ファイアウォールを設定してください。

■退職者のアカウントが残っていませんか？

近年、システム上に退職者のアカウントが残っていたために、不正アクセスを受けるという事件が発生しています。退職者のアカウントは、即時抹消するようにしてください。

■誰が、いつ、どの情報にアクセスしたか、
その記録はありますか？

適切な情報管理が行われていることは、記録によって確認されるものです。誰が、いつ、どの情報にアクセスしたか記録を取り、確認できるようにしてください。

■個人情報には必要最小限の社員のみが
アクセスできる仕組みになっていますか？

近年起きている個人情報漏えい事件の中には、個人情報にアクセスする必要のない社員が個人情報を漏えいしてしまった例が散見されます。漏えいの可能性を小さくするため、必要最小限の社員のみが、必要最小限の情報にのみアクセスできるようにしてください。

■社外に持ち出すPCやUSBメモリを紛失した場合でも
情報が漏えいしない対策がされていますか？

個人情報漏えいの原因として多いものは、紛失・置き忘れや盗難です。不要な情報を持ち出さず、また、情報を持ち出す場合には暗号化を施し、これらが原因となる個人情報漏えいを防止してください。