Sasanami & Partners

笹浪総合法律事務所

笹浪総合法律事務所

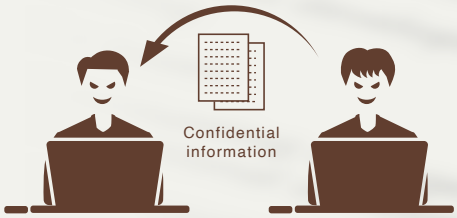
〒100-0005 東京都千代田区丸の内2丁目2番1号 岸本ビルヂング4階402号室
TEL：03-6213-0511　FAX：03-6213-0512　MAIL：office@sasanami-law.com
URL http://www.sasanami-law.com

2023 Winter
No.13

表紙写真：東京国際フォーラム

Column 01

退職者による秘密の持ち出しにご用心



弁護士　亀ヶ谷 貴之

取締役を務めた株式会社の原価情報などの仕入データを持ち出したことで、大手外食チェーンK社のT社長が逮捕されました。

T氏は、別の大手外食チェーンHを運営するZ社に退職の意向を伝え、秘密保持契約を締結していたにもかかわらず、部下に指示して、Hの仕入データを外部のサーバ経由で入手していました。また、K社への移籍後も、元同僚に、Hの毎日の売上データを送信させていました。

今般、T氏は、売上データではなく、仕入データの持ち出しを理由に逮捕されましたが、この点は、不正競争防止法が定める「営業秘密」の定義が関わっています。

1 「営業秘密」の定義

1)　「営業秘密」とは、①秘密管理性、②有用性、③非公知性の3要件を満たす必要があります（不正競争防止法2条6項）。

2)　本件における売上データ及び仕入データはいずれも、一般に知られた情報ではなく（③非公知性）、また、事業活動に有用な情報（②有用性）といえます。

3)　今回、仕入データ持ち出しが先に刑事事件化されたのは、売上データよりも仕入データの方が「①秘密管理性」の要件が認められやすいことが理由です。

経済産業省の「営業秘密管理指針」によれば、秘密管理性は、「企業が秘密として管理しようとする対象（情報の範囲）が従業員等に対して明確化されることによって、従業員等の予見可能性、ひいては、経済活動の安定性を確保する」ために求められるとされています。

この点、従業員への明確化のために、一つ一つの情報にまで、営業秘密かどうかを明記することは求められておらず、各企業の規模や業態等に即した媒体の通常の管理方法に即して、従業員において営業秘密か否かを判断できれば足ります。

例えば、ファイルや電子データ上にマル秘を付記するといった一般的な方法だけでなく、営業秘密については、パスワードを設定して限られた社員だけが把握できるようにすれば、秘密管理性が肯定される方向に働きます。

4)　今回の事件では、仕入データの閲覧は、一部の社員だけがパスワードを利用して行うことができ、売上データよりも秘密管理性が高いと考えられたことで、先行して捜査され、起訴に至ったと考えられます。

2 民事訴訟について

営業秘密の持ち出しについては、令和3年5月、大手通信会社S社を退職した社員が、他の通信会社であるR社に次世代通信規格に関する営業秘密を持ち出した件に関して、S社が、R社及び持ち出しを行った元社員に対し、1000億円の損害の一部として、10億円の支払を求める裁判を起こしました。

今回のT氏による営業秘密の持ち出しについても、民事の損害賠償請求がなされる可能性は高いと考えられます。

3 再発防止策

1）秘密保持契約書締結の意義

本件は、秘密保持契約を締結していたにもかかわらず、営業秘密が持ち出されており、単に秘密保持契約を締結するだけでは不十分でしたが、それでもなお、退職者との間で秘密保持契約を締結することは重要です。

これには予防の意味があるだけでなく、「秘密情報だとは思わなかった。」、「情報を持ち出してはいけないとは思わなかった。」といった言い逃れを防止する効果があります。

2）情報へのアクセス権限の管理等

ファイルへのアクセス権限や退職者が生じた場合のパスワードの変更などのルール作りをするなどの対策も必要です。

具体的には、従業員の退職の際、退職者のシステム利用IDやアクセス権限を削除する時期（退職者は退職に向けた準備の中で情報を持ち出すことが多いことに留意が必要です。）や手順等を事前に定めておき、退職者が出た場合にはそのルールに従って手続をとることが有用です。

3）従業員の教育

今回の事件は、T氏が、部下や同僚に対して秘密情報の送信を求めたものでした。そこで、従業員に対して、アクセス権限のない者から秘密情報を送信するよう求められても、拒否する旨回答させるように徹底させるなど、平時からの教育も非常に重要です。

Column 02

もう一歩進めましょう、情報セキュリティ対策

事務局　髙田 絵理（令和4年度上期情報セキュリティマネジメント試験合格）

新型コロナウイルスの世界的な流行を境に、私たちの仕事のやり方や生活様式が一変しました。その中でも特に大きく変化したのはテレワークに代表される働き方の変化です。それに伴い「情報」の価値が急上昇し、サイバー攻撃も急増、その手口も多様化し、企業は自社の情報資産※を守るため、その対策に追われています。

企業における情報セキュリティ対策の基本は、各個人のモラル意識に頼ることや同調圧力に甘んじることではなく、最低限守るべき明確な統一基準の設定・開示を行うことです。情報セキュリティ事故が起きた後で、信頼の回復に努めるのは容易ではありません。まずは、自社の現状を理解し、各組織に適した情報セキュリティ対策を進めることが肝要です。

※情報資産には「紙」「データ」いずれも含みます。

1 「情報セキュリティ」とは

企業にとって重要な情報資産を、①外部からのサイバー攻撃、②内部からの情報流出、③物理的資産の破損による情報の喪失から守ることを「情報セキュリティ」といいます。近年では、内外部からの脅威に対して適切にリスクアセスメントを実施して、企業における総合的な情報セキュリティを確保するため「ISMS（情報セキュリティマネジメントシステム）」の構築・運用が必須事項となっています。

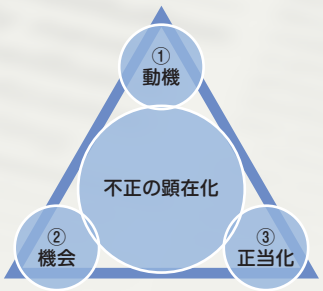
2 守るべき情報資産の特定と管理方法

ステップ1　自社の情報資産とその保管場所の把握
ステップ2　「機密度」と「重要度」で優先順位を設定
ステップ3　施錠、アクセス制限など適切な管理方法を決定
ステップ4　最悪の事態を想定し、管理方法が適切か検証
ステップ5　「機密度」と「重要度」を定期的に点検

IPAのホームページに掲載されている「5分でできる!情報セキュリティ自社診断」も是非お試しください。
https://www.ipa.go.jp/security/keihatsu/sme/guideline/5minutes.html

3 内部からの情報漏洩はなぜ起こるのか ～不正のトライアングル理論～

情報は、外部に持ち出された時点で、広く流通するリスクがあるため、持ち出させないための仕組み作りが重要です。内部からの情報の漏洩は、①「動機」②「機会」③「正当化」の3つの条件が揃った際に、発生しやすいと言われています。このうち、企業が対策できるのは、②の「機会」のみです。具体的には防犯カメラを設置する、重要なデータには、アクセス制限をかける、キャビネットは施錠し、鍵は上役が保管する、メールやサーバーのログをとる、紛失の危険のあるUSBなどへのデータの保存や社内セキュリティの範囲外の場所（個人で契約しているクラウド）などへのファイルの保存は認めないなどの対策が考えられます。



4 最後に

情報資産を取り扱うすべての人は、自社の機密情報が流出した場合の最悪の事態を想定して、その対策や手順を共有しておきましょう。

万が一に備えてサイバー保険に加入する、UTM（統合脅威管理）を導入するなどハード面での対策とともに、「情報セキュリティ規程」において、情報資産の取り扱い方法を分かりやすく文書化し、社内に周知することもぜひご検討ください。

当事務所では、「情報セキュリティ規程」の作成に付随する各種社内規程の見直しや改訂などを多角的・総合的な観点からアドバイスができる体制を整えております。情報セキュリティ対策をご検討の際には、迷わず当事務所にご相談いただければと存じます。

参考サイト

「情報処理推進機構」
https://www.ipa.go.jp/security/index.html
「情報処理マネジメントシステム認定センター」
https://isms.jp/index.html
「サイバーセキュリティ体制構築・人材確保の手引き」
https://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf