営業秘密官民フォーラムメールマガジン掲載コラム　第41回

営業秘密における秘密管理性と情報セキュリティ

弁護士知財ネット
弁護士　足立 昌聡

１．はじめに

ある情報が、不正競争防止法上の「営業秘密」として保護されるには、その情報が有用であって、公然と知られていないものであることのほかに、その情報が秘密として管理されていること（いわゆる「秘密管理性」）が必要です。

そして、過去の裁判例において、この「秘密管理性」の秘密管理性が認められるためには、企業の「特定の情報を秘密として管理しようとする意思」が、具体的状況に応じた経済合理的な「秘密管理措置」によって、従業員に明確に示され、結果として、従業員がその意思を容易に認識できる必要があります。

もっとも、ここでいう「秘密管理措置」には、経済産業省の「営業秘密管理指針」で示されているような、法律上の「秘密管理性」が認められる最低限のレベルのものから、同様の「秘密情報保護ハンドブック」で示されているようなベストプラクティスといえるレベルのものまで幅があります。

ところで、近年では、営業秘密のほとんどがデジタルな情報として「電磁的」に管理されています。そこで、本稿では、営業秘密における「秘密管理措置」とは、情報セキュリティにおけるどのような対策と関連するのかをご紹介します。

２．情報セキュリティの３原則

情報の秘密とは、情報に対するアクセスがコントロールされている状態が保たれていることをいいます。情報セキュリティの世界では、ある情報が知るべき者以外に知られていない状態のことを、「機密性（Ｃｏｎｆｉｄｅｎｔｉａｌｉｔｙ）」が確保されているといいます。この情報を知るべき者だけが情報にアクセスできるべきという考え方を「Ｎｅｅｄ　ｔｏ　Ｋｎｏｗ」の原則といい、情報に対するアクセス制御の基本となります。

また、情報が不正確であったり、不完全であったりすると、その情報の価値は毀損されてしまいます。そこで、情報が価値を保つには、その情報が正確かつ完全である状態を維持している必要があり、このような性質を「完全性（Ｉｎｔｅｇｒｉｔｙ）」といいます。

ところで、ある情報を１００％安全に守る方法は、その情報へのアクセスを完全に遮断

してしまうことです。しかし、アクセスを完全に遮断することは、開ける方法がない金庫のようなもので、そこに収められているものの価値を無にしています。そのため、アクセス制御は、その情報が利用可能な状態にあることを維持している必要があります。これを「可用性（Ａｖａｉｌａｂｉｌｉｔｙ）」といいます。

以上の情報の機密性、完全性及び可用性は情報セキュリティの３原則とされ、その頭文字をとって「ＣＩＡ」と呼ばれています。それでは、実際にどのようにＣＩＡを確保するのかを見ていきましょう。

３．アクセス制御

１）識別

情報に対するアクセスを許可すべき者とそうでない者を区別するには、最初に、アクセスしようとする者が何者であるのかを識別（Ｉｄｅｎｔｉｆｙ）する必要があります。例えば、会社に新しく従業員が入社すると、その従業員に社員番号などの識別子（Ｉｄｅｎｔｉｆｉｅｒ）を付与し、これを用いて従業員を識別することになります。

逆に言えば、ある識別子に対して与えられたアカウントを複数人が使い回している状態では、識別子はアクセスしようとする者を区別する手段としては機能していません。従って、このようなアカウントの使い回しを許容しているシステムは、形式的にはアクセス制御を実施しているようにみえても、従業員側から見れば形骸化しており、不正競争防止法の適用においても、秘密管理措置を認識しうる情況にないと評価されるおそれがあります。

２）認証

次に、情報にアクセスしようとする者が、自分は従業員Ａであると名乗っている際に、その人物が本当に従業員Ａであるかを確認する必要があります。このプロセスを認証（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ）といい、例えば、識別子とパスワードの組み合わせで行う方法などがあります。

ところで、パスワードが認証に利用可能なのは、そのパスワードを知っている者が、そのパスワードと紐付いた識別子で識別される者本人のみであるという場合に限られます。従って、パスワードが全員同じであるとか、パスワードが識別子やその他の容易に知りうるユーザの属性（誕生日等）である場合には、パスワードを本人しか知り得ないとはいえません。従って、このようなシステムも、形式的にはアクセス制御を実施しているようにみえても、秘密管理措置を認識しうる情況にないと評価されるおそれがあります。

なお、認証には、知識認証（パスワード等）のほかに、所有物認証や生体認証のような方法があります。まず、所有物認証とは、銀行のＡＴＭにおいて、キャッシュカードの持

参人を本人とみなすような方法があたります。加えて、生体認証は、指紋や虹彩などの同じ特徴を持つ人が極めてまれなものを利用する方法です。

キャッシュレス決済事業者における事故で話題となった「２段階認証」とは、同じ要素認証を２つ組み合わせてセキュリティを高める方法で、例えば、パスワードのほかに合い言葉を尋ねる方法は、知識認証という同じ要素を２段階で利用しているので、２段階認証に当たります。一方、銀行のＡＴＭにおける認証は「２要素認証」と呼ばれ、キャッシュカード（所有物認証）と暗証番号（知識認証）という異なる要素を組み合わせてセキュリティを高めています。

３）認可

最後に、認証された者にどのような権限を与えるのか決定するプロセスを「認可（Ａｕｔｈｏｒｉｚａｔｉｏｎ)」と言います。例えば、ある者へ、あるデータベースを閲覧することだけができる権限と、そのデータベースの内容を編集することができる権限のいずれ、または両方を付与するなどの決定が認可に当たります。

不適切な認可の一例としては、業務効率を優先するあまり、すべての従業員に管理者（Ａｄｍｉｎｉｓｔｒａｔｏｒ）の権限を付与してしまうケースです。この場合は、従業員からすれば、自分に万能な権限が付与されていることから、どのようなことも自分には許されていると受け取ってしまうリスクがあります。このようなケースでは、従業員が秘密管理の意思を認識しうるとは評価されないおそれが強いといえます。

４．役割によるアクセス制御

営業秘密が漏えいした過去の事例では、退職者が在職中のアカウントを退職後も利用可能であったために、退職後に情報が持ち出される事案が散見されます。このような事故は、ある従業員が退職又は異動をしたという情報が人事系のシステムには反映されていても、情報資産を管理するシステムに反映されない隙をついて起きています。

社外からのアクセスを制限することはもちろんですが、認可される権限（Ａｕｔｈｏｒｉｔｙ）の範囲を、従業員の役割（Ｒｏｌｅ）に連動させると、権限管理が容易になります。例えば、財務系の部署に所属した従業員が特許管理系の部署へ異動した場合、その従業員の識別子（社員番号）でアクセス権限の範囲を管理していると、人事異動の情報をタイムリーにキャッチアップして、情報資産管理のシステムのアクセス権限を更新する必要があります。しかし、予め「財務」や「特許管理」という役割にアクセス権限の範囲を設定しておけば、人事系のシステムの「役割」の更新を参照することで、容易に権限管理を行うことができます。最終出社日後、有給休暇の消化期間中はアカウント自体は給与支払い等の事務手続のために維持する必要があったとしても、「役割」を更新しておけば、この

間隙を突いた情報の持ち出しを防ぐことができます。

５．おわりに

本稿では、主にアクセス制御の手法が営業秘密の秘密管理とどのようにかかわるかを紹介しましたが、営業秘密のみならず、法改正で新しく導入された「限定提供データ」においては「電磁的管理性」が保護要件とされていることから、より情報セキュリティの確保が重要となります。また、個人情報保護法上の安全管理措置のように、事故の発生が行政処分や刑事罰につながるようなケースも起こりえます。情報セキュリティにおいては、基本の３原則を忘れずに、常に最新の情報を入手し、情報セキュリティへの適切な投資を行うべきでしょう。

以上