営業秘密を保護するためにはどうしたら良いか

知財よもやま話　第 11 話

柿　沼　太　一

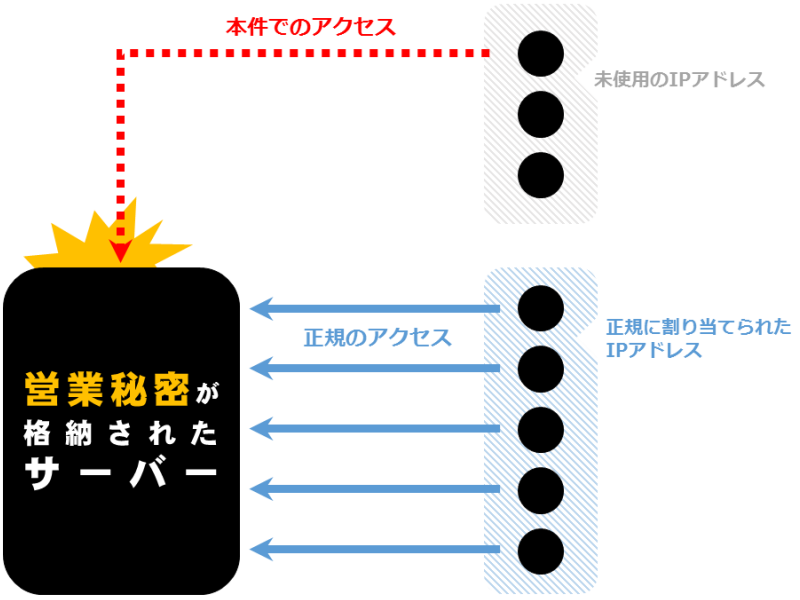
１．あるチャット

「私のところでは日本の技術を手に入れることができる」
「あなたが売れる人を探すなら、連絡費用２０万あげます」
「提供できるのは設計図一式＋３Ｄファイル」
「これは盗んできたものです」
「捕まったら処断される」
「私が自分で売れば、多く稼げる」
「しかし危険が大きい」
「こんな危険なこと、一般的な１年分の年収で、日本野郎はみんなやりたがらないよ」
「私たち半分ずつ分けても良いですよ」

これ、何だと思いますか。
ある大手企業で、社員による営業秘密の漏洩が行われ、不正競争防止法違反で刑事事件化したのですが、その社員が外部の人間に秘密を売り込むために交わしたチャットです。
今回は、この「ヤマザキマザック事件」（名古屋地裁平成２６年８月２０日判決）を題材に不正競争防止法における営業秘密について考えてみたいと思います。

２．事件のあらまし

・社内ファイルサーバーのフォルダ内に技術データが電子ファイル形式で保存されていた。
・それらのデータには業務上必要が認められる部署の従業員がアクセス、ダウンロード可能。
・従業員に貸与された業務用パソコンを起動するのに必要な ID、及び従業員個人が設定するパスワードの認証によってネット ワークにアクセスする権限を有する従業員であるかどうかを部署単位で識別、照合。
・ネットワークに接続した端末を識別するためにパソコン 1 台ごとに異なる IP アドレスを割り当てていたが、どの端末にも割り当てられていない空き IP アドレスが存在。
・被告人は、自己のパソコンに割り当てられた IP アドレスを空き IP アドレスに変更してデータにアクセスしてデータを複製。



３．営業秘密として保護されるためには

この事件の争点はいろいろあるのですが、本件は不正競争防止法違反事件ですので、被告人が複製したデータが不正競争防止法上の「営業秘密」かどうかが問題になります。

不正競争防止法の「営業秘密」は、
① 秘密として管理されている［秘密管理性］
② 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［有用性］であって、
③ 公然と知られていないもの［非公知性］
と定義されています（不正競争防止法２条６項）。

実務的に問題になることが多いのは、このうち「秘密管理性」です。
たとえば、
・「営業秘密」といいながら、他の情報と区別されていない。
・パスワードも設定されておらず誰でもアクセスできる状態だった
・印刷された秘密情報ファイルが入ったキャビネットが無施錠
などの場合には、秘密管理性が否定されることもありえます。

不正競争防止法の「営業秘密」についての詳細は、平成２７年１月に改定された「営業秘密管理指針」と、平成２８年２月に公表された「秘密情報の保護ハンドブック」（これは、

秘密情報の漏えい防止・漏えい時に推奨される様々な対策例を紹介したものです）を参照してください。

【営業秘密管理指針】
http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/20150128hontai.pdf
【秘密情報の保護ハンドブック】
http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf

営業秘密管理指針では、「秘密管理性」について
（１）営業秘密保有企業の秘密管理意思（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ていること。
（２）その結果として、従業員が当該秘密管理意思を容易に認識できる（換言すれば、認識可能性が確保される）こと
が必要であるとされています。

４．ヤマザキマザック事件における「秘密管理性」
そしてヤマザキマザック事件でも、やはりこの「秘密管理性」が争われました。

（１）諸規定は整備されていた
この事件では、以下のように諸規定は整備されていました。

- 情報管理に関する事項として、会社内外を問わず、機密性のある情報等を第三者に開示、漏洩、提供してはならない旨が就業規則に規定。
- 事業部ＨＰの上部には、閲覧者全員に対して、「当社は、このホームページにて開示された技術情報に関する権利を所有し、当社の事前の許可無く、その全部または、一部を問わず第三者に開示してはならない。尚、このホームページにアクセスした者と閲覧した情報は履歴管理されている事を承知した上で活用する事。」との警告文が表示
- 平成１５年２月１７日策定の電子情報セキュリティ規定で、「業務遂行上止むを得ない場合を除き、クライアントＰＣや各種媒体への複製及び出力を禁止する。」、「業務遂行以外の目的で可搬記憶媒体へコピーをしない。」などと規定。

（２）しかし実際の運用に若干ルーズな時期があった
もっとも、秘密管理性の判断においては、各種規定があるだけでは不十分で、実際にきちんと運用されていたかが問題となります。

営業秘密管理指針でも「情報に対する秘密管理措置がその実効性を失い「形骸化」したともいいうる状況で、従業員が企業の秘密管理意思を認識できない場合は、適切な秘密管理措置とはいえない。」とされています。

この点、この事件においては、実際の運用に、以下のように若干ルーズな時期がありました。

- 被告人が平成１８年１１月から所属した営業技術部アプリケーショングループでは、全て会社貸与の外付けＨＤ８個とＵＳＢメモリ１２個が使用されていたが厳格な管理は行っておらず、いわゆる貸しっぱなしの状態だった。
- 平成１９年６月から所属した同部金型グループでは、当初、全て会社貸与の外付けＨＤ１個とＵＳＢメモリ３個が使用され、特定の従業員に貸しっぱなしの状態であった。

（３）運用の改善

このような運用のままであれば、もしかしたら秘密管理性は否定されたかもしれません。

しかし、そこで運用を改善したのが、A 営業技術部長でした。

A 営業技術部長は、部内における外部記憶媒体の乱用を問題視して以下のような施策を矢継ぎ早にとりました。

- 外部記憶媒体の使用を管理するよう指示する内容のメールを各グループリーダー宛てに発出
- その指示に基づき、外部記憶媒体はグループリーダーが管理するとしたルールを定め、外部記憶媒体をリストアップした上、管理台帳により、その貸し出し、返却等を管理し、個人所有の外部記憶媒体の持ち込み、使用を禁止するなどした。
- その結果、同部において「フラッシュメモリ及び外付けハードディスクの管理表」と題する管理台帳やＵＳＢメモリ管理ルール及び携帯型メモリ管理ルールなどが運用・策定された。
- その後は、外部記憶媒体は管理台帳によって管理されて使用されるようになっていた。

加えて、本件では、以下のようなルールの周知がなされていたこともあり、本件では無事「秘密管理性」が認定されました。

- 新人研修の際に法務部門の担当者から各種規定について説明され、被告人の入社時にも、同様に説明が行われた。
- 新規にルール等が策定されたり、改訂されたりした場合には、電子掲示板で周知されていた。
- 携帯型メモリ管理ルール等について、被告人も参加したグループミーティングにおいて所属従業員に周知された。

５．秘密管理措置の具体例

この事例からわかるように、「このような措置をとっていれば確実に秘密管理性が肯定される」という一義的な答えはありません。

もっとも、先程来ご紹介している営業秘密管理指針には、秘密管理措置の具体例として以下のような例が列挙されていますので参考までに紹介いたします（もっとも、この具体例は「ここまでやらなければ秘密管理性が認められない」という意味ではなく、一つの例に過ぎません)。

・対象文書に「マル秘」など秘密であることを表示
・個別の文書やファイルに秘密表示をする代わりに、施錠可能なキャビネットや金庫等に保管
・紙媒体のコピーやスキャン・撮影の禁止、コピー部数の管理（余部のシュレッダーによる廃棄)、配布コピーの回収、キャビネットの施錠、自宅持ち帰りの禁止措置
・記録媒体へのマル秘表示の貼付
・電子ファイル名・フォルダ名へのマル秘の付記
・営業秘密たる電子ファイルを開いた場合に端末画面上にマル秘である旨が表示されるように、当該電子ファイルの電子データ上にマル秘を付記（ドキュメントファイルのヘッダーにマル秘を付記等）
・営業秘密たる電子ファイルそのもの又は当該電子ファイルを含むフォルダの閲覧に要するパスワードの設定
・記録媒体そのものに表示を付すことができない場合には、記録媒体を保管するケース（ＣＤケース等）や箱（部品等の収納ダンボール箱）に、マル秘表示の貼付
・人事異動・退職毎のパスワード変更、メーラーの設定変更による私用メールへの転送制限、物理的に USB やスマートフォンを接続できないようにすること等

これらの具体例や、先ほどの「秘密情報の保護ハンドブック」に紹介されている方法を参考に各社において合理的な秘密管理措置をとることをお勧めいたします。