営業秘密官民フォーラムメールマガジン掲載コラム 第53回

「米国企業が提供するクラウド型サーバに保管された秘密情報の持ち出し行為に対する証拠収集としてのディスカバリの活用」

弁護士知財ネット
弁護士　山岡裕明

米国企業が提供するクラウド型サーバに秘密情報を保存する機会が増えているのではないでしょうか。例えば、Microsoft社のクラウド型サーバOneDriveに秘密情報に係る電子ファイルを保存する場合や、SaaS企業がソフトウェアプロダクトに係るソースコードをAWS（Amazon Web Services）やGCP（Google Cloud Platform）などのクラウド型プラットフォームのサーバに蔵置する場合が考えられます。

こうしたクラウド上のサーバに保存された電子ファイルが内部者又は外部者（元従業員を含む。）により不正に持ち出された場合、持ち出した者を特定するにあたりIPアドレスを含むアクセスログが重要になります。

ところが、プロバイダ責任制限法４条１項に規定される発信者情報開示請求は、不正アクセスによる権利侵害を対象としていないと解されます[1]。
そうすると、アクセスログの収集は警察による捜査に委ねざるを得ませんが、米国企業がクラウド型サーバを提供している場合、一般的には、刑事共助条約（Mutual Legal Assistance Treaty）に基づいて、米国の捜査機関に捜査共助を要請することになるところ、米国が受けた共助要請については、共助完了までに平均して約10か月掛かるとされています[2]。これでは、一定期間の経過をもって消去されるIPアドレスなどの証拠については捜査が間に合わない可能性があります。

そこで、有用な手段となり得るのが、米国の証拠開示制度であるディスカバリです。

一般的に、ディスカバリは、米国で民事訴訟を提起した後に、公判審理（トライアル/Trial）

[1] プロバイダ責任制限法４条１項は「特定電気通信による情報の流通によ」る権利侵害を対象としており、「特定電気通信」とは「不特定多数の者によって受信されることを目的とする電気通信」（同法２条１号）であるところ、不正アクセス行為は、この「不特定多数の者によって受信されることを目的とする電気通信」による情報の流通を伴うものではないため。
[2] PRESIDENT'S REVIEW GRP. ON INTELLIGENCE & COMMC'NS TECHS., LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS 227（2013）

の前に実施される証拠開示手続です。トライアルの準備のため、法廷外で当事者主導のもと、お互いに事件に関する情報を開示し収集する手続のことです(連邦民事訴訟規則 26 条等)。

これは、原被告間で実施されるものなので、米国における訴訟提起及び訴訟係属を前提とします。

ところが、このディスカバリの特則として民事手続合衆国連邦法典第 28 編 1782（a）（標題「外国及び国際法廷並びにその当事者のための援助」）があり、この制度を利用することで、米国で訴訟提起を予定していなくても、日本において訴訟提起を予定する者は、簡易迅速に米国企業からアカウント情報の開示を受けることが可能となっています。すなわち、証拠収集のためだけに、相手方を予定しない（一方当事者による）申立を裁判所に行い、裁判所が認容命令を発令した場合、命令書と必要書類をいわゆるコンテンツプロバイダに送付することで、当該プロバイダから証拠開示を受けることができます。

そして、プロバイダ責任制限法と異なりディスカバリには侵害行為の限定はありません。また、申立から開示に至る期間も最短で 1 か月程度です。

したがって、ディスカバリを活用すれば、上記の手続の難点を見事にクリアできます。

当初はインターネット上の誹謗中傷及び著作権侵害の事例において活用してきたディスカバリですが、他の事案への応用可能性が開けてきました。今後、秘密情報の持ち出し事案において、証拠収集の一つの有力な手段として活用される機会も増えるのではないかと期待しています。

以上