米国企業等との取引における情報コンタミネーションリスクへの対策

弁護士知財ネット
外国法事務弁護士・米国弁護士　一色太郎

1　はじめに

オープンイノベーションの取り組み等において取引先から秘密情報を受領する機会が増す中、情報コンタミネーションリスクが高まっている。

情報コンタミネーション（以下、「情報コンタミ」または「コンタミ」）とは、他社技術等の外部秘密情報が自社情報に混入した状態を指す。情報コンタミが発生すると、自社開発等において使用可能な情報の特定が困難となり、他社営業秘密の不正使用リスクが高まる。

本稿では、米国法の観点から、取引先から受領した秘密情報に関する情報コンタミリスクとその対策について検討する。なお、情報コンタミは、新規採用者が前職で得た秘密情報を転職先企業に持ち込むこと等によっても発生するが、本稿では取引先から適正に受領した秘密情報に関するコンタミリスクに絞って解説する。

2　情報コンタミリスクとは

2.1　秘密情報受領に伴うあらゆる局面で発生し得る問題

取引契約においては、受領秘密情報は、契約が定める目的に限って使用が認められるのが一般的である。情報コンタミは、目的外使用制限を伴う形で秘密情報を受領するあらゆる局面で発生し得る問題であり、例えば、以下のような局面が想定される。

① 共同開発目的で受領した秘密情報を自社開発に用いること。
② 出資または買収検討に際しターゲット企業から受領した秘密情報を自社事業開発に用いること。
③ 受託製造において顧客から受領した秘密情報を他社向け製品の開発・製造に用いること。
④ 技術ライセンスに基づき受領した秘密情報を自社の別製品の開発に用いること。
⑤ コンサルティングサービス提供時に受領した秘密情報を他社向けのサービス提供に用いること。

これらの行為は、目的外使用を禁じる契約違反のみならず、受領秘密情報が「営業秘密」である場合、営業秘密の不正使用にあたる。米国法においては、他者の営業秘密を不正に取得、使用または開示することは、営業秘密の「窃取」（misappropriation）とされ、秘密保持契約等に基づき適正に取得した営業秘密を契約の許諾範囲を超えて使用することは営業秘密の窃取に該当する[1]。

2.2　情報コンタミを取り巻く環境

取引先から技術情報等を受領する機会はあらゆる企業において存在するが、十分なコンタミ対策を講じている国内企業は少数とされる[2]。コンタミ対策を講じる国内企業が少ない理由として、主

[1] *See* 18 U.S.C. §§ 1831-1839.
[2] 独立行政法人情報処理推進機構「企業における営業秘密管理に関する実態調査」67頁（2017年3月17日）

に以下の三つが考えられる。

1. リスク認識の欠如：秘密保持契約（NDA）等に基づき秘密情報を受領する時点では、将来の目的外使用を想定しておらず、よって、コンタミリスクが認識されないことが多い。情報コンタミリスクは、事業戦略や開発方針の変更等により、契約が認めていない自社開発等の目的で取引先情報を使用する際に顕在化する。しかし、その時点では、契約締結からかなりの時間が経過していることが多く、取引先情報が使用制限を伴っていることを現場の開発担当者らが把握していないこと等が少なくない。
2. 「ブラックボックス」内の出来事：製品開発に用いられた情報がどのようなものであったのかは内部関係者にしか分からない。このため、情報コンタミの発生状況は外部からは判別困難であり、よって、情報コンタミは「ブラックボックス」内の出来事とされる。仮に情報コンタミが発生しても、その事実が発覚しないこともあり、「どうせバレない」と高を括っているケースもあると思われる。
3. 秘密裏の紛争解決：取引関係のあった企業間で発生するコンタミ紛争は、当事者間の話し合いまたは当該契約が定める仲裁手続によって解決が図られることが多い。いずれの場合も、コンタミ紛争が発生していること自体が公にならないため、紛争リスクが過小評価される傾向にある。

公正取引委員会は「スタートアップの取引慣行に関する実態調査報告書」の中で、目的外使用等の NDA 違反が疑われるコンタミ事例を紹介している[3]。公取は、「NDA に違反してスタートアップの営業秘密を盗用し、スタートアップの取引先に対し、スタートアップの商品・役務と競合する商品・役務を販売することにより、スタートアップとその取引先との取引が妨害される場合には、競争者に対する取引妨害（一般指定第 14 項）」にあたると指摘している。公取の報告は、国内においても情報コンタミが相当数発生していることを示唆している。

2.3 米国企業等との取引におけるコンタミリスク

米国企業や大学との取引における情報コンタミリスクは、国内企業との取引と比べ格段に高い。

その理由として、米国訴訟は比較的容易に提起可能であり[4]、いったん訴訟提起されると、ディスカバリー手続において「ブラックボックス」がこじ開けられ、自社開発において参照した情報等を含む、広範な文書開示が命じられることが挙げられる。

さらに、米国訴訟では、地域市民から無作為に選出される陪審員が事実認定を行うのが一般的である。情報コンタミ訴訟において、被告は「営業秘密」の公知性や対象製品の独自開発を主張する。一方、原告は、被告を信頼して営業秘密を開示したにも関わらず、被告に裏切られた、といった主

（https://www.ipa.go.jp/files/000057774.pdf）。本調査によると、共同・受託研究開発実施時の対策については、25%の企業が「情報授受の際に秘密保持契約を締結」しているが、その他の対策についてはいずれも 1 割未満の企業でしか実施されていない。

[3] 公正取引委員会「スタートアップの取引慣行に関する実態調査報告書」39 頁（事例 7）、49 頁（事例 43）（2020 年 11 月）（https://www.jftc.go.jp/houdou/pressrelease/2020/nov/201127pressrelease.html）。

[4] 営業秘密訴訟の提起に際しては、①原告が被告に営業秘密を開示したこと、②被告の製品情報等から原告の営業秘密が不正に用いられたと考えられることを訴状に記すだけでよく、不正使用を示す確定的な証拠は必要とされない。*See, e.g., Bell Atl. Corp. v. Twombly*, 550 U.S. 544 (2007) (A complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face.).

張をすることが多い。原告代理人の語る「信頼と裏切り」といったヒューマンストーリーが陪審員の心に響きやすく、被告に不利となる傾向がある。特に、ベンチャーや中小企業が大企業を相手取る訴訟はその傾向が強いとされ、時に陪審は驚くほど高額な損害賠償を言い渡すことがある。

以下は、NDA に基づき開示を受けた秘密情報の不正使用に関する訴訟事例であり、米国企業との取引におけるコンタミリスクの高さを如実に表している。

2.4 【事例紹介】米国企業からの秘密情報受領に伴うリスク

Mitsubishi Electric & Electronics USA（以下、「MEUS」）の担当者は、2001 年、シリコンバレーの半導体ベンチャーGrail Semiconductor（以下、「Grail」）の創業者らと面談した。その当時、Grail は資金繰りに困っており、投資家を探していた。

面談に先立って Grail は秘密保持契約（NDA）の締結を要求した。MEUS は、受領秘密情報を Grail の承諾なしに使用すること等を禁ずる NDA に署名した。面談時に、Grail はパワーポイントを用いたプレゼンを行い、三種類の半導体メモリ（DRAM、SRAM、フラッシュ）の利点を組み合わせる新型メモリのアイデアを開示した。MEUS は Grail への投資を見送った。

2004 年、資金が底をつき休眠会社となっていた Grail は、ルネサスエレクトロニクス（日立製作所と三菱電機の合弁会社で 2003 年設立）が開発した新型メモリの紹介記事を目にした。Grail は、記事で紹介されているルネサスの新型メモリは、Grail が開示した技術情報を不正使用して開発されたものであると主張し、2007 年、MEUS を NDA 違反、営業秘密侵害等を理由にカリフォルニア州地方裁判所に提訴した。

2012 年、陪審は MEUS による NDA 違反を認定し、124 百万ドルの支払いを命じた。その後、カリフォルニア州控訴裁判所は、陪審による損害額算定に誤りがあったとして再トライアルを命じた[5]。再トライアル前に和解が成立（和解内容は非公開）。

3 情報コンタミ対策

コンタミ対策は、取引先との間で締結する契約内容をどうすべきかという側面と、契約締結後の対策に分けられる。本章では、取引先と受領秘密情報の目的外使用を禁じる契約を締結した後の対策について解説する。なお、本稿で論じる対策は、米国企業や大学との取引に限らず、国内で完結する取引であっても有効である[6]。

3.1 自社保有情報の日時確定

取引先から技術情報の開示を受けた後に、独自に類似技術を開発したことを証明するためには、自社開発において受領秘密情報を用いなかったことを示すことが求められる。一方、取引先から秘密情報を受領する前に当該技術を保有していたことを示せれば、取引先の情報に依拠せず開発したことの立証が容易となる。

このため、取引先から秘密情報を受領する前に、自社が保有する関連情報を特定し、それらが存

---

[5] *Grail Semiconductor, Inc. v. Mitsubishi Electric & Electronics USA, Inc.*, 225 Cal.App.4th 786 (Cal. Ct. App. 2014).

[6] 情報コンタミ対策については、経済産業省「秘密情報の保護ハンドブック」（2016 年）にも詳しく記されている（第 5 章「他社の秘密情報に係る紛争への備え」参照）。
（https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf）。

在していた日時を確定すべきである[7]。日時確定方法には、公証制度の活用、特許出願、ラボノートへの記載に加え、電子文書に日時情報を付す「タイムスタンプ」の活用等がある。

3.2 受領プロセスの明確化

コンタミ紛争は、秘密情報を受領してから何年も経過してから発生することが多い。よって、後に受領秘密情報を特定できるよう、受領プロセスを明確化し、受領情報をしっかりと管理することが欠かせない。

メールでの受領に際しては、プロジェクト用のメールアドレスを設定し、その窓口を介して受領することが望ましい。担当者個人のアドレスを窓口とした場合、担当者が退職してしまうと受領情報の全容確認が困難となるため、特定個人に依拠しない仕組みを構築することが重要となる。また、打ち合わせ時に紙媒体で渡された情報等については、受領情報の概要、受領日時および経緯を記すログを作成すべきである。

なお、契約目的とは関係のない秘密情報の受領は避けるべきである。例えば、共同開発を行っている際に、別の技術に関する情報共有の提案がなされたとする。一見問題のなさそうな情報であっても、目的外使用を禁ずる契約において受領する技術情報が、自社の他部門が進めている技術開発等に制約を及ぼす可能性がある。(仮に不要な情報を受領してしまった際には、当該情報を返却または廃棄し、その旨を記録として残し、コピー等が社内で拡散しないよう対策を講じる必要がある。)

3.3 分離保管およびアクセス制限

自社情報と他社情報が混在してしまうと、後に他社の秘密情報を使用していないことの立証が困難となる。よって、他社の秘密情報は、自社情報と分離して保管すべきである。

他社秘密情報は、自社情報とは別のフォルダ（またはサーバー）にて管理し、分離管理されたフォルダには関係者以外がアクセスできないようすべきである。後に、権限のない者によるアクセスがなかったことを示せるよう、アクセスログ等の記録を残すことも重要である。

他社秘密情報へのアクセス者が増えるにつれ、不正使用等のリスクが高まる。よって、他社秘密情報を「知る必要のある者」を特定し、その者のみにアクセス権を付与すべきである。紙媒体の資料については、他社秘密情報が記載されていることが容易に識別できるようした上で、特定のファイルキャビネット等に施錠して保管する。

3.4 受領秘密情報の廃棄対応

受領秘密情報およびその派生情報については、契約終結時に廃棄または返還が求められるのが一般的である。

廃棄作業は多くの困難を伴う。例えば、取引先の秘密情報がバックアップシステム等に保存されることがあるが、これらのシステムは一部の情報のみを選択的に廃棄できないよう設計されていることが多い。さらに、社員の個人メールに含まれる取引先秘密情報の廃棄も必要となるが、これらの廃棄作業は各社員に委ねられるのが一般的である。彼らが関連するメールやファイル等をもれなく廃棄したことの確認は困難であり、廃棄されたはずのメール等が米国訴訟のディスカバリー時に

[7] 技術情報の日時を確定する手続きは「技術封印」ともいう。

「発見」されることがある。

情報コンタミのクレームを受けた際、まず、受領秘密情報を特定し、それらを自社開発等に用いなかったことの確認が必要となる。契約終結時に受領秘密情報をすべて廃棄してしまうと、紛争時に受領情報の特定ができなくなり、不正使用等の判断が困難となる。このため、契約において、受領情報を記録目的で１セット保管することが明記されることがある。

仮に契約が保管を明示的に認めていない場合であっても、記録用に１セット残すことを検討すべきである。そして記録用データは法務・知財部門が厳格に保管し、契約終結後、誰もその情報にアクセスしなかったことを示せれば、開示者側に実損は生じないことから、損害賠償リスクを制限することができる。

3.5　自社開発時の対策

情報コンタミリスクは、他社との共同研究開発テーマと類似する内容の研究開発を、自社単独または別の他社と共に行う際に格段に高まる。自社開発等へと舵を切ることで、それまでの共同開発パートナーは競合へと変貌を遂げるためである。

このため、類似技術の開発等を行う際には、より踏み込んだコンタミ対策が必要となる。自社で独自開発を行う際の対策を以下に記すが、別の他社との共同開発等においても同様の対策が求められる。

3.5.1　自社開発メンバーの選定

コンタミ対策の観点からは、他社との類似技術開発に関わった者を自社開発に関わらせないことが好ましい。当該契約が「残留情報」（無意識に記憶の一部と化した情報）の使用を認めていない場合、他社秘密情報を知る者が自社開発に関わることで、コンタミリスクを排除できなくなるためである。

しかしながら、類似技術の開発経験者を自社開発から外すという選択肢は現実的ではない場合がほとんどであろう。他社秘密情報にアクセスした者が自社開発に参加する場合は、自社開発環境のスクリーニング対策が特に重要となる。

3.5.2　自社開発環境のスクリーニング

自社開発環境に外部秘密情報が混入すると、コンタミリスクは大幅に高まる。例えば、自社開発メンバーが、元共同開発パートナーの秘密情報を含むメールを保有していた場合、同メンバーがそのメールを参照しなかったことを立証するのは極めて困難となる。

米国訴訟では広範な証拠開示が命じられ、「独自開発」を主張した場合、不正使用が疑われる技術の開発経緯に関する担当者のメール等が開示対象となる。自社開発メンバーが、取引先の秘密情報を保有していた場合、不正使用を裏付ける直接的な証拠がなくとも、不正使用が推定されるリスクが生じる。

このため、自社開発を行うにあたっては、自社開発メンバーがアクセスしうる情報源（サーバー、個人フォルダー、紙ファイル等）のスクリーニングを行い、そこに外部秘密情報が含まれないことの確認が必要となる。取引先から受領した文書やデータそのものに加え、それらに言及する内部資料やそれらに依拠して作成された資料等もスクリーニングの対象とすることが求められる。

3.5.3 クリーンルーム対策

さらに踏み込んだ対策として、自社開発に使用する情報を事前にフィルタリングし、自社開発を外部秘密情報の保管建屋から物理的に離れた場所で行う「クリーンルーム」対策がとられることがある。

リモートワークが進む今日では、開発を物理的に離れた場所で行うことの意義は薄れているが、自社開発において使用する情報を事前にフィルタリングし、自社開発に用いた情報を明確化にし、開発経緯について記録化することで、独自開発の立証はより容易となる。

3.5.4 誓約書の取得

自社開発を行うにあたっては、自社開発メンバーから、他社秘密情報を開発に使用しない旨等を書面で確認すべきである。

例えば、X 社との共同開発後に、類似技術について自社開発を行う場合は、自社開発メンバーから、「X 社秘密情報を保有していないこと」、「自社開発において X 社秘密情報にアクセスしない」旨を記す誓約書を取得する。さらに、X 社との共同開発に参加したメンバーからも、X 社秘密情報を今後一切開示・使用しない旨を定めた誓約書を取得することで、共同開発メンバーと自社開発メンバーとの間で X 社秘密情報のやり取りがなかったことの主張が強化される。そして、自社開発終了時には、自社開発および共同開発メンバーの双方から確認書を取得し、誓約が遵守されたことを確認する。

誓約書および確認書を取得することは、誓約内容が遵守されたことの立証にはならないが、当該社員にコンタミ対策の徹底を促すとともに、踏み込んだ対策を講じたことの証拠となる。仮に X 社が情報コンタミの可能性を指摘した際に、誓約書等を取得したことは、不正使用がなかったことの状況証拠となる。

———

コンタミはブラックボックス内の出来事であるため、取引先からクレームを受けた際、不正使用がなかったことについて合理的な説明ができないと訴訟・仲裁に発展するリスクが高まる。アクセス制限、スクリーニング、誓約書取得といった対策を講じたことを伝えることによって、取引先との紛争がエスカレートすることを未然防止する効果が期待できる。

3.6 【事例紹介】技術情報の受領を拒否したキヤノンの対応

以下に、米国企業からの技術情報提示を拒否したキヤノン（株）の事例を紹介する。本事例は、当時キヤノン知財部長であった丸島儀一氏が自著『キヤノン特許部隊』において紹介しており、情報コンタミリスクの本質と対策の重要性を言い当てている [8]。

1980 年代、米国のハネウェル社はオートフォーカス技術を開発し、日本のカメラメーカー各社に売り込んだ。売り込みに際してハネウェルは、①オートフォーカスのモジュールおよび②関連技術情報の開示を提案し、②関連技術情報については技術評価目的以外での使用を禁じる NDA の締結を要求した。

この売込みに対し、ミノルタは①モジュールと②関連技術情報を入手し、検討を行ったが、ハネ

[8] 丸島儀一『キヤノン特許部隊』120-124 頁（光文社新書、2002 年）。

ウェルの技術は採用せず、自らオートフォーカスを開発した。後に、ミノルタはハネウェルから、特許侵害、契約違反および営業秘密侵害で訴えられ、一審敗訴後、128 百万ドル支払うことで和解した[9]。

ハネウェルはキヤノンに対しても同様の売り込みを行った。その際、キヤノンは①モジュールだけを入手し、目的外使用制限が課された②関連技術情報の受領を拒否した。

この判断について、丸島氏は次のように述べている。

> 特許権の訴訟だけだったら、特許を使っているかどうかというのは、特許権というはっきりとしたものがあるし、現物もあります。ところが技術情報を使った使わないという場合、使わなかったという立証も難しいし、使ったという立証も難しいのです。しかしアメリカの裁判は陪審裁判です。一般のアメリカ人には、日本人はアメリカの技術を真似するんだという感覚が刷り込まれている。そういう土壌でこの微妙な訴訟を起こされたら、とても勝ち目はない、と私は思っていました。ですから評価のための契約の時にそんな機密保持契約を結ぶと、事業部の活動を制約することになると判断し、キヤノンは違う契約にしてもらったのです。
>
> ・・・
>
> 事業部の人は、そのとき欲しいものは欲しい。だから契約書を作ってくれ、とくるわけです。しかしそのとき、将来的な技術動向や会社の動きをみて、こういう問題が発生するぞということを特許担当者が指摘できるかどうかが重要です。そのことを議論した上で、それでも欲しいというならばもらって厳重な管理をしなければなりません。しかし一口で厳重な管理といっても、それにはまた大変な問題があります。ひとつ間違うと、企業活動を大きく制限する結果になるのです。

4　おわりに

コンタミ対策を講じる際には、対策の負の側面にも配慮が必要である。企業は、目的外使用を禁ずる NDA 等の契約を日常的に締結している。契約義務の遵守は重要であるが、外部秘密情報を一律に厳格に管理することのコストは高く、過度なコンタミ対策は、開発スピードの劣化や社内横断的な情報共有の阻害要因ともなり得る。

このため、コンタミ対策のレベルは事業リスクを踏まえ調整すべきである。同一内容の契約であっても、例えば、相手が米国のベンチャー企業の場合と、長年にわたる取引関係のある日本企業の場合とでは、紛争化するリスク、そして紛争が事業に及ぼしうるリスクは大きく異なる。よって、誓約書の取得等の踏み込んだコンタミ対策は事業リスクの高い事案に限って行う、というのも一案であろう。

本稿が、効果的な情報コンタミ対策のあり方を模索する企業の参考となれば幸いである。

---

[9] Reuters, *Minolta Settles Suit on Honeywell Patents*, N.Y. Times, March 5, 1992. (https://www.nytimes.com/1992/03/05/business/company-news-minolta-settles-suit-on-honeywell-patents.html)