

無許諾知財の使用に対する米国の 不公正競争防止法を通じた対策

アーサー・M・ミッチェル*

抄 録 多くの米国企業や日本企業は、知的財産権および情報技術の開発に関して優位な立場にあります。アジアのサプライチェーンにおける「無許諾知財」の使用は、その優位な立場を脅かすものです。この脅威への対策として、既存の州法および連邦法が従来とは異なる新たな方法により適用され、また新たに法案が成立するなどの動きがあります¹⁾。

Q 1 「無許諾知財」とは何ですか。またどのような問題点がありますか。

A 1 情報化時代において、あらゆる知的財産権（特許権、商標権、著作権、意匠権および営業秘密を含む、以下「知財」という）は、米国企業や日本企業にとって最も重要な財産の一つです。故意の「ライセンスの不正使用」がなされた場合（たとえば、10のライセンスについての費用負担のみで、1,000の設備で使用）、またはライセンスフィーが全く支払われずに、その正当な権利者以外の者により製品の製造過程で知財が使用された場合、もしくは自身の製品または部品に含めることにより使用された場合、正当な権利者および正当に許諾を受けたライセンサーは、競争上不利な立場に陥ります。また、知財の盗用が明らか場合もあります。無許諾知財とは、このように、何らかの不正もしくは違法が介在している知財またはその問題です。

グローバル化により、米国、日本および欧州の主要な企業は、より安価なサプライチェーンの供給業者を見つけることでコストを最小限に抑える方法を模索する必要性が生じています。ほとんどのアジア諸国の知財法制は、無許諾知財

の使用を違法としていますが、実際には、当該法令の執行は緩やかで、無許諾知財を使用する者やそれに関わる者を規制しきれておりません。そのような者は、合法的に知財を利用する競争事業者と比較し、コスト面で、競争上、不当に優位に立つこととなります。これは、米国企業にとって非常に大きな問題で、米国国家安全保障局長は、コンピューターネットワークを通じた知財または産業情報の盗用やスパイ活動を「史上最大の富の移転」と表現しています。

Q 2 米国の不公正競争防止法は、どのような背景事情のもとで制定されたのですか。

A 2 1938年、連邦取引委員会法（FTC法）第5条により、不公正・欺瞞的な行為または慣行が禁止されました。1970年代～1980年代には、多くの州が、主に消費者を欺瞞や不公正な行為から保護するために、FTC法第5条をモデルにした法令（「Baby FTC Acts」）を成立させました。現在、すべての州およびコロンビア特別区において、不公正・欺瞞的な行

* ニューヨーク州弁護士、元アジア開発銀行
ジェネラルカウンセル Arthur M. MITCHELL

為および慣行（以下「UDAP」という）に関する規制がありますが、衡平法上の救済（すなわち、差止命令）、損害賠償または不当利得の返還、違約金の可否および訴訟提起の当事者適格については、州により多種多様です。最近では、ワシントン州およびルイジアナ州がそれぞれUDAP法を修正し、情報技術の盗用に対する具体的な救済の規定や、一定の場合、盗用情報技術が関与する製品から利益を享受する第三者（すなわち、自らが違反行為を行った供給業者以外の者）が責任を負う代理責任の規定を定めました。

Q 3 どの州法が適用されますか。

A 3 州により、UDAP法の具体的な内容、法令の解釈、執行方法や執行状況が異なるため、どのような無許諾知財の案件に、どの州法が適用されるかを類型化することは極めて困難です。もっとも、後述のカリフォルニア州やマサチューセッツ州の最近の動向によると、州司法長官や無許諾知財の使用により影響を受ける米国の産業は、その産業を保護するために当該規制を適用できるか検討しているようです。すべての州およびコロンビア特別区のUDAP法において、州当局（通常は、選挙により選ばれた司法長官）に当該規制の執行権限が与えられています。さらに、私人による民事訴訟または集団訴訟（クラスアクション）を認めている州もあります。

また、すべての州およびコロンビア特別区は、営業秘密の盗用を違法とする規制を定めています。最近では、DuPontから営業秘密を盗用した韓国企業に対する多額の損害賠償（9億1,990万ドル）案件において、バージニア州の営業秘密法に基づき、損害賠償および差止命令請求が行われました。

Q 4 どの連邦法が適用されますか。

A 4 消費者保護の管轄当局である連邦取引委員会(FTC)は、FTC法第5条に基づき、あらゆる不公正・欺瞞的な行為に対し執行権限を行使できます。なお、現在までに、FTCが、無許諾知財や盗用情報技術に関して執行権限を行使した案件はありませんが、州の司法長官により構成される連合会(National Association of Attorneys General)や米国議会の委員会は、FTCに対し、かかる案件に対する執行を要請しています。米国の法律関係者らは、FTC法第5条は他の法令では捕獲できない法的な問題を解決することができると考えています。

1930年関税法337条は、米国内の産業が「毀損されるか、著しい損害を受ける」場合、またはそのおそれがある場合の「製品を輸入する際の不公正な競争や行為」を禁止しています。国際貿易委員会(ITC)は、特許権、著作権、商標権、意匠権を含む米国の知財を侵害する一切の製品の輸入を排除できます。また、同法は、営業秘密の不正利用が米国外で行われた場合であっても、かかる不正使用によって製造された製品が米国に輸入される場合に適用されると解釈されています。

さらに、連邦経済スパイ法(Economic Espionage Act)は、金銭上の利益または外国企業の利益のための営業秘密の盗用を、連邦犯罪と規定しています。

Q 5 どのような新しい対策が検討されていますか。

A 5 2013年5月7日、著名な上院議員から成る超党派グループは、「サイバー盗用抑止法」法案を提出しました。この法案が可決された場合、国家情報長官は、(i)サイバー空間で、米国企業・個人に対して経済および

産業スパイ活動に携わる外国のリスト、(ii) 盗用された情報を利用して製作された製品のリスト、ならびに(iii) 盗用から利益を享受した国有企業を含む外国企業のリストなどを作成することが必要です。本法案は非常に広範囲で、盗用財産から「利益を享受する」サプライチェーンのすべての者が対象となり得ます。本法案は、該当する一切の製品を米国から排除するための権限を大統領に付与するものです。

Q 6 侵害品を米国から排除できますか。

A 6 排除可能です。違反製品(の一部)が米国から排除されることは、違反者にとって最も深刻な制裁です(なお、違反行為に対する制裁はQ7参照)。ほぼすべての州およびコロンビア特別地区のUDAP法のもとで、裁判所は、衡平法上の救済(差止命令)を命ずることができます。実際、輸入禁止が求められ、またそれが認められる可能性は高いといえます。連邦レベルでは、FTC法が差止めによる救済を定めており、また関税法337条の手続では「限定的」または「一般的な」排除命令を明確に認めています。サイバー盗用抑止法のような法案が制定されると、大統領は、行政手続として違反製品を阻止する権限を有することとなります。

Q 7 違反行為が証明された場合の制裁には、どのようなものがありますか。

A 7 制裁の内容は、州により多種多様です。違反者は、補償的損害賠償(さらに、2倍または3倍損害賠償が認められる場合がある)、懲罰的損害賠償、差止命令、排除措置命令、民事制裁金、弁護士報酬、外部監査の裁定額を命じられ、また報告義務を課される場合があります。法違反に対する故意ないし意図が要件ではない州法もあります。ほとんどの州規制は、非常に広範囲で、裁判所に「不公正な行為」ま

たは「欺瞞的な行為」と認定されるほぼすべての行為を含むことから、違反行為による部品を完成品に組み込んだ第三者も射程範囲内となります。多くはありませんが、製造業者に対するセーフハーバーを規定する州法もあります(ワシントン州法等)。FTC法は、違反を知っていたことに対する民事制裁金に加え、排除命令などの差止命令(関税法337条の手続でも可能)を定めています。

Q 8 実際の案件や想定される事案には、どのようなものがありますか。

A 8 現在までに明らかとなっている案件は多くはありませんが、現状を考慮すると、これらは氷山の一角に過ぎないでしょう。〈州レベルの事案〉

・2012年10月、タイにある魚介類加工業者に対し司法長官が提訴したマサチューセッツの案件(ナロン・シーフード事件)は、同加工業者による制裁金(10,000米ドル)の支払い、同加工業者が今後米国内に販売する自社の商品に関して無許諾のソフトウェアを使用しないこと、および同加工業者による継続的なITシステムの内部監査義務を条件に、和解が成立しました。

・2013年1月、カリフォルニア州司法長官は、同州のUDAP法に基づき、カリフォルニア州で販売された衣類の製造過程で盗用ソフトウェアを使用したとされるインド(Pratibha Syntex, Ltd.)および中国(Ningbo Beyond Home Textile Co.)企業を提訴しました。違反が認定された場合、一つの違反行為につき最大で2,500米ドルの制裁金が課されます。何をもって一つの違反行為と認定されるかにより、制裁金が莫大となる可能性もあります。

・テネシー州司法長官は、2013年6月、タイのタイヤ会社が関連する不公正競争行為に対し、執行権限を行使しました。

・ワシントン州司法長官は、マイクロソフト

のソフトウェアのライセンスの不正使用に関し、ブラジル企業であるEmbrarerと1,000万米ドルで和解に至りました。

＜連邦レベルの事案＞

サプライチェーン関連において、無許諾知財に関する連邦レベルの執行や訴訟（関税法337条手続を含む）は、州レベルよりも頻繁に行われています。

・前述Q3のとおり、バージニア州連邦裁判所は、「Kevlar」のフォーミュラを不正利用した韓国企業に対し、州の営業秘密法を適用し、莫大な金額の損害賠償および厳格な差止命令を命じました。

・また、裁判所は、中国で不正利用された営業秘密を用いて製造された製品を米国に輸出した中国企業（TianRui Group）について、関税法337条の違反行為が認定しました。

Q 9 特に注意すべき点および対処法は？

A 9 日本企業は、アジアのサプライチェーンにおいて、極めて広範囲、かつ複数のレベルで供給業者に依存しているため、危険にさらされています。前述のとおり、サプライチェーンに無許諾知財が介在することの故意や意図の有無にかかわらず、規制の対象となり、損害賠償請求義務が発生する場合は少なくありません。気づかぬうちに無許諾知財に関与してしまっている日本企業が、当該製品を米国に輸出する場合、莫大な制裁金が科され、また米国への輸出を禁じられることもあります。世界的に競争が激化するにつれ、州司法長官が、現地の産業を保護するため、既存の法律を新たな方法で施行することも想定されます。連邦当局もまた、世論を受け、アジア諸国における盗用知財の取締りを強化するものと思われます。

アジアのサプライチェーンへの依存は高まるばかりであり、対応を怠ると、リスクも高まり

ます。既に一部の企業は、事業に深刻な崩壊を引き起こすリスクを回避するため、不良品、安全、環境、人権侵害および腐敗防止について、自身のサプライチェーンを監視しています。無許諾知財がサプライチェーンに含まれることを防止するためにかかる費用は、金銭的・風評損害や事業の中断による損害と比較すると、はるかに少額であるといえます。

Q 10 以上のリスクに関して、日本企業はどのような対策をとるべきでしょうか。

A 10 以下の5つのポイントが特に重要と考えられます。

1. まずは、サプライチェーンの状況を把握することが重要です。現在採用しているサプライチェーンに関するコンプライアンス対応に、無許諾知財への対策も含めることが、潜在的なリスクを回避する第一のステップとなります。
2. 取引先と契約する際、取引の相手方に、無許諾知財に関与していないことを表明保証してもらい、契約書にその旨の表明保証条項を明記すべきです。この他、契約書には、取引先の無許諾知財の関与により生じ得る損害賠償額の予定額を予め定めておくことや、実際に損害が生じた場合の貴社の免責条項などを定めておくことによっても、リスクを軽減できます。
3. 特に購買やリスク管理に関わる従業員や得意先、供給業者に対し、コンプライアンス研修を行うことによって、それらの者が、潜在的な問題を察知できるようになり、無許諾知財に関与するリスクを軽減することができます。
4. コンプライアンス方針を公表すること、また同業者団体と協力して無許諾知財の撲滅のために適切な活動をすることにより、供給事業者による無許諾知財への対策が期待できます。
5. 新たな基準、規則、ベストプラクティスを作ることに、協力すること。

本文の複製、転載、改変、再配布を禁止します。

注 記

- 1) 本記事で触れた問題については、アーサー・M・ミッチェル，洞雞敏夫，丹羽正爾，大軒敬子，NBL, No.999, pp.34～41 (2013) も参照されたい。

(原稿受領日 2013年8月26日)

