Vol.2016-EIP-71 No.9
2016/2/19

不正競争防止法
営業秘密保護規定 2015 年改正に関する一考察

須川 賢洋[†1]

概要：今回の不正競争防止法の改正は、最近の事件や国際状況に合わせて、営業秘密の漏洩・拡販に対する刑罰を重くするとともに、顧客名簿などの個人情報保護強化も視点に置いたものだと言える。それらについて考察する

キーワード：不正競争防止法，営業秘密，情報セキュリティ

Unfair Competition Prevention Act ,
A study of trade secret amendment on 2015

Masahiro SUGAWA[†1]

Abstract: Revision of the current unfair competition act , according to the recent incidents and international situation , as well as heavier penalties for leakage , sales of trade secrets , personal information protection strengthening , such as customer roster also said that the thing you put in perspective . It is considered them

Keywords: Unfair Competition Prevention Act, Trade secret, Information securty]

1. はじめに

2015 年（H27 年）7 月に不正競争防止法が改正され、主に営業秘密漏洩防止への強化が図られた。この改正法は 2016 年（H28 年)1 月 1 日より施行されている。本稿ではこの改点について考察することとする。

不正競争防止法（以下、不競法）は、通常は 2.3 年に一度の改正が行われているが、前回の改正が 2011 年（平成 23 年）であり、過去 5 回の改正に比べれば、多少ではあるが間が開いたものとなった。これは、従前の改正、特に 2009 年(H21 年)時の改正で、営業秘密漏洩に関してはかなりの部分をカバーするようになり、一応の安定を得たと言えようことが大きいと思う。

不競法も、他の法改正の例に漏れず、社会や産業に影響を与えた大きな事件が契機となり改正されることが多い。2009 年改正は、いわゆる「デンソー事件」1をきっかけとしており、2011 年改正は、携帯ゲーム機の技術的制限手段を回避する機器として「マジコン」のようなものが広く流通した結果行われた。そして今期改正は、2015 年春に起きた、「ベネッセ事件」に負うところが大きい。そして、ヤマザキマザック、新日鉄などといった企業から海外への先端技術が持ち出されたことがこれに続く。

†1 新潟大学

2. 改正点

今回の改正は、営業秘密の保護強化に主眼をおいたものであり、前述のとおり、昨年発生したベネッセからの大量の個人情報持ち出し事件をはじめとして、海外メーカへ国内の先端技術の流出が相次いだことをきっかけとして強化されたものである。むろん、デンソー事件のように今までも海外への悪意ある営業秘密の流出はあったわけだが、外国人によるものだけでなく、日本人が海外企業への転職などの際にも情報を持ち出すことが目立つようになったことを看過してはならないであろう。この問題は、法律の問題だけにとどまらず，雇用政策や団塊世代の大量リタイアと就業年齢層の変化などにも起因しており、抜本的解決の為には、これらの問題も考察せねばならないが、本稿の目的とは異なるため割愛する。

しかしながら、今回の改正の特徴的なところの一つとして、主管庁である経済産業省は、こういったインパクトのある事件をその改正の解説の全面に打ち出していることが挙げられると言えよう。

今回の改正項目を筆者の見解に従いざっと羅列すると以下のようになる。

1. 罰金の引き上げ
2. 海外犯への重罰化
3. 犯罪収益の没収

ⓒ2016 Information Processing Society of Japan

4. 不正開示された情報を取得した者を処罰可能に
5. 非親告罪化
6. 未遂罪の追加
7. 海外蔵置のクラウド・サーバへの対応
8. 侵害の立証負担の軽減
9. 営業秘密侵害製品の輸出入の禁止
10. 消滅時効の延長

経済産業省の公表資料ではこれらを、(1)刑事上・民事上の保護範囲の拡大、(2)罰則強化等による抑止力の向上、(3)民事救済の実効性の向上の三つに大きく分類している。

(1)刑事上・民事上の保護範囲の拡大
・営業秘密の転得者処罰の範囲拡大
・国外犯処罰の範囲拡大
・未遂行為の処罰
・営業秘密侵害品の譲渡・輸出入等の規制

(2)罰則強化等による抑止力の向上
・罰金刑の上限引上げ等
・犯罪収益の任意的没収規定の導入
・非親告罪化

(3)民事救済の実効性の向上
・損害賠償請求等の容易化（立証負担の軽減）
・除斥期間の延長

といった項目順になる。

ベネッセ事件での、顧客名簿の転売問題対策を政策的に前面に押し出したのではなかろうかと類推できる。

3. 各改正項目の略説

3.1 罰金の引き上げ

もっとも分かりやすい改正点であるが、営業秘密侵害行為に関する罰金額が引き上げられた。現在は、個人の場合で最高 1,000 万円、法人の場合で最高 3 億円であるが、これが個人で 2,000 万円以下、法人で 5 億円以下となる。

懲役刑のほうは今回は引き上げられていないので、営業秘密侵害に関する量刑は結果として「十年以下の懲役若しくは二千万円以下の罰金に処し、又はこれを併科する」ということになった。

この罰金の引き上げの限らず、今回の改正では、特に刑罰が強化されていることが特徴である。その為、罰則を定める第 21 条が大幅に修正・追加されている。21 条関係の改正が大部分を占めるといっても過言ではない。

3.2 海外犯への重罰化

興味深いのは、「海外重課」という仕組みが取り入れられたことである。これは営業秘密を海外で使用する目的で侵害したり、海外で使われる事が分かっていて漏洩したりした場合、海外で不正に使用した場合などに、国内での場合より重い刑罰を課すもので、海外への漏洩に対しての罰金額は個人で最高額 3,000 万円、法人で 10 億円の罰金となる。（注意：懲役の量刑は変わらず。）

3.3 犯罪収益の没収

近年では、「犯罪で得た財産や報酬は没収してしまうべきだ」という考え方が積極的に取り入れられており、また国際的にも主流となっている。本法でもこれを規定した。もしある企業が仮に、違法に入手した営業秘密で 10 億円の利益を得た場合には刑事立件されて罰金を払ってもなお 5 億円の利益が残ってしまうわけであり、これも回収してしまおうというわけである。

3.4 不正開示された情報を取得した者を処罰可能に

現在の法律では、営業秘密を不正に取得・漏洩した者と、それを知りながら営業秘密をその者から直接開示を受けた者（つまり、二次入手者）までしか取り締まることができない。ベネッセ事件の際に問題になったのがまさにこの点であり、不正に取得された顧客名簿だと分かっていてそれを名簿業者から買って DM 発送を行ったりする者、更に再販売する別の名簿業者などは処罰の対象とできなかった。今回の改正では、このような転々流通した営業秘密の取得・使用・開示者も処罰の対象となった。

3.5 非親告罪化

現在の営業秘密侵害罪は、被害者の告訴をもって行われる親告罪であるが、これを非親告罪とした。これによって、捜査・逮捕の迅速性が期待できる。

3.6 未遂罪の追加

文字通り。未遂行為も新たに刑事罰の対象になったわけであるが、この効果は大きいと予想できる。未遂行為は取得の未遂と開示の未遂に分けられ、例示として、経産省の例としては、以下のものが挙げられている2。

Ex.)
・*不正アクセス行為は確認されたが、証拠の隠滅等により営業秘密たる情報の持ち出しの事実を確認できなかった場合。*
・*社内メールシステムの管理者の地位を利用し、社内幹部宛のメールが自動で自らにも転送されるようなプログラムを埋め込んでいたが、実際に営業秘密情報が転送される前に明るみに出た場合。*
・*営業秘密を電話で売り込み、その後メールで営業秘密を不正に開示するべく、送信しようとしたが、メールソフトの不具合により転職先に到達しなかった場合。*

3.7 海外蔵置のクラウド・サーバーへの対応

日本国内で事業を行う企業の営業秘密を海外で取得し

ⓒ2016 Information Processing Society of Japan

た場合も刑事罰の対象となることが明文化された。海外のサーバに保管して管理していた情報が搾取された場合などを想定している。

以下は主に民事面での改正となる。

3.8 侵害の立証負担の軽減

営業秘密のうち、設計図や生産技術などの技術情報の場合、そもそも相手先企業が情報を不正取得したということを証明すること自体が困難である。そこで、それら秘密技術の使用が疑われる製品を生産した場合に、一定の条件の下に、営業秘密を侵害したと推定する規定が追加された。

3.9 営業秘密侵害製品の輸出入の禁止

これは営業秘密を侵害していることを知っていた場合に限定されるのだが、その営業秘密を侵害した品を譲渡したり引き渡したりすることも禁止された。この条文の追加と併せて関税法も改正され、この規定に関しては輸出・輸入に対しても適用される。もちろん、電気通信回線を通じての提供の際も該当する。この行為に関しては差し止め請求が認められ、さらには刑事罰の対象にもなっている。上記(1)と同じ量刑になる。

3.10 消滅時効(除斥期間)の延長

これあまり大きく取り上げられていないてんではあるが、営業秘密の侵害の停止又は予防を請求できる期間、つまり営業秘密の不正使用の差し止め請求可能期間が、「事実を知った時から 3 年・行為の開始の時から 10 年」→「事実を知った時から 3 年・行為の開始の時から 20 年」に延長されている。このことは非常に大きいな意味を持つと言える。先端技術が複雑化・専門化し、かつ、」その保管や閲覧にデジタルデバイスが使われるようになり、ストレージの大容量化、クラウド化がイベントの検出事態に遅延を生じさせる結果となっている。また海外メーカによる模倣は細部までを知るには時間がかかることもある。よって時効延長は大変望ましいことであろう。

4. 考察

4.1 転得者処罰範囲の拡大について

繰り返し述べているとおり、今回の改正の最大のきっかけが 2015 年春に起きた通信教育会社ベネッセでの顧客名簿の不正持出である。

この事件では、システム保守を担当する子会社のエンジニアが、金銭目的で名簿業者に顧客情報を売りわたしている。このような競業他社への漏洩が目的ではなく、自己の利益とせんところのいわゆる「図利加害行為」に関しては、平成 21 年度（2009 年）改正（施行は 2011 年 7 月 1 日）にて既に刑事罰規定が設置されていたため3逮捕・起訴は問題なく行えたわけである。

しかしながら、本事件が発覚後もっとも問題視されたことは、営業秘密の持出ということ事態よりも、それによって流出した 3000 万件とも言われる顧客情報（個人情報）のその後の流通である。従来の不競法では、営業秘密を不正に取得・漏洩した者と、それを知りながら営業秘密をその者から直接開示を受けた者（つまり、二次入手者）までしか取り締まることができない。

名簿業者の手に渡ってしまった名簿を、ベネッセより流失したものだと知った上でなお購入したり、あるいは名簿自体を取引したりされている実態が判明したわけであるが、従前はこれらの三次・四次取得した者に対して、刑事的な規制を加えることができなかった。これを可能にしたものである。つまり、不正に取得された顧客名簿だと分かっていてそれを名簿業者から買って DM 発送を行ったりする者、更に再販売する別の名簿業者などは処罰の対象とできなかったわけである。

これを指し示す言葉として『「転々流通」した営業秘密の取得・使用・開示』という言葉が使われている。「転々流通」はもともと貨幣の特徴などを表するときに使う言葉であるが，情報を価値ある財とみなせばこれを営業秘密に使うことは非常に親和性が高いと言える。

つまるところ、今回の改正では，個人情報保護法を保管して個人情報の更なる保護を図ることが目的の一つであったとも言えよう。むろん、2015 年に改正された個人情報保護法でも個人情報の保護は強化されたわけであるが、営業秘密に占める情報のうち、従来は技術情報が中心だったものが、顧客名簿などの営業情報の占める割合、またその価値が増大したことを鑑みるに不競法においても個人情報を保護しておくことは有益だと言える。

経産省の後方資料ではこの改正点が一番最初に記載されており、いかにこの点に重点を起き、また国民への理解を得ようとしたかが見て取れる。

4.2 量刑について

量刑の変更に関しては、通常は懲役も加算しさらに罰金を増やすというやり方が取られるが、今回は罰金の増額のみにとどまっている。しかしながら、知的財産権の主たる法律、つまり特許法4や著作権法といった一連の知的財産権を定める法律での、侵害罪の上限が懲役 10 年であることを考えると，営業秘密漏洩に関する罪のみ懲役刑をさらにそれより加重することは甚だ不都合と言える。これらの法改正と合わせて行う必要があるであろうが、刑事法政の観点からは、懲役の上限が 10 年でも既にかなりの重い罪であり、

今後これをさらに引き上げるためには、他の犯罪の刑罰とのバランスを考慮する必要が生じるであろう。

不正競争防止法の刑罰は、営業秘密侵害に関する主たる罪状は、その量刑の上限を懲役 10 年、罰金 1000 万円としているが、元来の不正競争の概念である商品等表示のタダ乗りや、原産地や品質の偽造等に関しては懲役５年、罰金 500 万円を上限としているものが多い。営業秘密だけに視点を当てた場合、昨今の各国の知財重視政策の中で国際的にもバランスのとれたものあるとは思われるが、法の本筋の部分を置き去りにして、一方的に量刑が増えているところもある。この点については、一考の必要があると考える。特に、本稿の趣旨とは一部論点が逸れてはしまうが、最近はこの表示の不正が、特に食品において多発しており、これらは人命に直結することもある。営業秘密保護が重要であることは言うまでも無いことであるが、量刑のバランスとして人命に関わることのほうが少ないという構成には疑問を持つ。将来的には条文としては、21 条に関して２項を廃止して１項のみとして、すべて同じ量刑とすることを提言する。横並びにしておいても、個々の裁判において事件の特性に応じて求刑すれば実害はないものと思われる。この方法が好ましくないのであれば、「罰則については特許法の量刑を準用する」というやり方もあるであろう。この方法の利点は、知財侵害の量刑バランスを保つことができ、国際ニーズに応えやすいことにある。

4.3　クラウド・サーバーに保管された営業秘密データの扱い

今回の改正では、たとえ国外のクラウド・サーバーに保管されている国内企業の営業秘密であっても保護されることが明確になったと言う点が強調されている。保護対象となる営業秘密を、「日本国内において管理されていたもの」から「国内において事業を行う保有者の」に変更された。「クラウド」という言葉が頻繁に使われるようになったことに考慮しているのであると思われるが、この点に関しては、私見では、従前も明文規定がなかっただけで決して法の効力範囲に入っていなかったことはないと考える。サイバー犯罪の取り締まりにおいては、従前より、国内で行為の一部がなされていれば国内法が適用されており、これが営業秘密関連の罪に関してだけ適用できないということないと考える。しかしながら明文化されている場合の安心感というものがことエンジニアや技術開発を中心とする企業においては強いことは想像に難くなく、営業秘密漏洩の舞台が大企業からサプライチェーンやステークホルダーに移りつつある現状においては、中小企業を意識した条文であると言えよう。

最大の問題は，クラウド経由で営業秘密が持ち出された時のその立証方法にあると言える。3.6 で挙げているように、たとえ営業秘密の持出の事実が確認できなくても、ログ等で不正アクセス行為が確認できれば未遂罪が適用できるわけであるが、現実には、クラウド・サーバーではこのログの確認すらできない場合が多い。筆者は従前より、侵害の証跡をはっきりと残すためにもデジタル・フォレンジックの営業秘密保護への積極的採用を主張しているが、海外やクラウド上への機密情報の保存を行う必要がある場合は、そのサーバの契約段階から、どのようなログが記録でき、またいざという時にどのような情報を契約当時者が直接に操作・入手可能かなのかを検討した上で利用する必要あろう。技術情報の場合はネットワーク上での蔵置はあまり行われないと思われるが、前述のとおり、営業秘密のうち顧客名簿などのサービス情報の重要性が高まったが故の今期の法改正であり、こういったサービス情報の場合はクラウド上にて保管される可能性がかなり高いと言え、実務としては、法律から約款、SLA（Service Level Agreement）に至るまで一貫した整合性を保つ必要が生じると言えよう。今回の 21 条 6 項の改正（追加）が十分な機能を果たすことができるかどうかについては、今後さらに検討しなければならない点も多くあると思われ、これについては今後の研究課題としたい。

---

1) 大手自動車部品メーカのデンソーにて、正規雇用の中国人技術者によって社内データベースから大量の技術情報がダウンロードされた事件。中国人技術者は DB へのアクセス権を持っていたため、不正アクセス禁止法を適用することはできず、また自身の研究の為に技術を入手したと主張したが為、当時の不正競争防止法を適用することができず、結果として起訴できなかった。

2）経産省提供資料「不正競争防止法の概要」
http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/27kaiseigaiyou.pdf

3)　法 21 条 1 項：十年以下の懲役若しくは千万円以下の罰金に処し、又はこれを併科

4) 同日に「特許法」の改正法案も成立しているが、今回は 35 条「職務発明」規定の修正に留められており、量刑の増加はなされていない。

ⓒ2016 Information Processing Society of Japan