

経済産業省委託

令和3年度重要技術管理体制強化事業（中小企業アウトリーチ事業（営業秘密漏えい対策））

2022年3月

独立行政法人 日本貿易振興機構

イノベーション・知的財産部

目次

[1] はじめに.....	2
[2] 個別支援.....	3
1. 概観.....	3
2. 個別支援企業.....	3
3. 個別支援企業へのアンケート結果	4
[3] 普及啓発.....	6
1. 概観.....	6
2. 個別支援企業募集セミナー	6
(1) 日本	6
(2) 中国	6
3. 成果普及セミナー.....	6
4. 技術流出防止管理説明会	6
[4] マニュアル作成.....	8
1. 概観.....	8

〔1〕はじめに

グローバル化により海外に進出する日系企業が増加し、それに伴い技術情報等の漏洩リスクも増大している。令和2年度の「企業における営業秘密管理に関する実態調査」では¹、9割以上の企業が「営業秘密の漏えいに関して脅威を感じているものがある」と回答しており、その中では「海外の拠点・取引先・連携先を通じた自社秘密情報の漏えいについて対策が必要と考えている」との声も聞かれ、海外での漏えいを防ぐ管理体制の整備が必要となっている。

一方、中小企業を中心に、海外拠点におけるリソースは限定されており、営業秘密管理の重要性認識や管理体制整備が不十分な企業は少なくない。営業秘密管理の重要性が認識されていない場合、競合他社の立ち上げ等自社ビジネスへの影響が出て初めて対応策を検討することになるが、既に流出してしまった秘密情報は取り戻すことができない。また、営業秘密管理の重要性を認識している場合でも、製造や労務管理等に忙殺され、管理体制の確立・整備にまで手が回らないケースも散見される。

そこで、本事業では、在外日系中堅・中小企業を主なターゲットにすえ、現地事情に精通した専門家によるハンズオン支援と情報提供・普及啓発活動による意識の底上げを通じて、これまでに蓄積した営業秘密漏えい事案に関する知見等を活用しながら、日本企業の営業秘密管理体制整備の支援を拡充させ、海外での技術・ノウハウの意図せぬ流出を防ぐことを目的として各種事業を実施した。

¹ 令和3年3月、独立行政法人情報処理推進機構（IPA）が公表
(<https://www.ipa.go.jp/files/000089191.pdf>)。同調査報告書 31 頁を参照。

〔2〕個別支援

1. 概観

中国に進出する日系企業は、32,000 社超と世界最多であるが、人材の流動性が高く、営業秘密流出に関する相談も多いことから、引き続き、本事業へのニーズが見込まれたため、昨年度より継続して中国を実施対象とした。また、近年、ASEANに進出する日系企業が増加しており、外務省の海外進出日系企業拠点数調査（令和2年）によれば²、日系企業の拠点数上位10ヶ国中5ヶ国をASEANが占めている。また、令和2年10月末～12月初にかけてJETROが実施した調査によれば、「今後、新たに海外進出したい」とする企業の比率は新型コロナウイルスの影響を受けてもなお微減にとどまっており、事業拡大先の2位にベトナム、4位にタイ、8位にシンガポールがあげられていたことから、ベトナム、タイ、シンガポールを本事業の実施対象とした。具体的には、営業秘密管理体制整備を希望する在中国日系企業11社、在タイ日系企業5社、在ベトナム日系企業5社に対し、現地の専門家により営業秘密管理状況のヒアリングを実施し、アドバイス（管理状況の改善、契約書等の改正案作成）、必要に応じて現場確認や従業員や管理職への研修等を行った。

2. 個別支援企業

（1）中国

	企業	支援先拠点	支援期間
1	A社	浙江省	8月16日(月)～2月16日(水)
2	B社	山東省	10月21日(木)～2月18日(金)
3	C社	上海市	8月10日(火)～2月18日(金)
4	D社	広東省	12月21日(火)～2022年2月10日
5	E社	江蘇省	11月11日(木)～1月18日(火)
6	F社	江蘇省	11月3日(水)～2月
7	G社	広東省	12月23日(木)～2月10日
8	H社	上海市	12月2日(木)～2月15日(火)
9	I社	上海市	11月23日(火)～2月18日(金)
10	J社	江蘇省	12月8日(水)～2月
11	K社	上海市	12月3日(金)～2月18日(金)

² 令和3年7月、外務省が公表

(https://www.mofa.go.jp/mofaj/ecm/ec/page22_003410.html?msclkid=3137ebb4ab4e11ecb704a268e6c3bc4f)。

(2) タイ

	企業	支援先拠点	支援期間
1	L 社	ラヨーン県	8 月 6 日(金)～2 月 2 日(水)
2	M 社	バンコク	8 月 9 日(月)～1 月 19 日(水)
3	N 社	バンコク	12 月 15 日(水)～2 月 18 日(金)
4	O 社	バンコク	8 月 31 日(火)～2 月 11 日(金)
5	P 社	チョンブリー県	8 月 3 日(火)～2 月 11 日(金)

(3) ベトナム

	企業	支援先拠点	支援期間
1	Q 社	ハノイ市	9 月 24 日(金)～2 月 18 日(金)
2	R 社	フンイエ省	12 月 9 日(木)～2 月 18 日(金)
3	S 社	バクニン省	11 月 11 日(木)～2 月 18 日(金)
4	T 社	ホーチミン市	12 月 8 日(水)～2 月 18 日(金)
5	U 社	フンイエ省	12 月 10 日(金)～2 月 18 日(金)

(4) シンガポール

応募企業なし

3. 個別支援企業へのアンケート結果

アンケート回答企業 20 社中、9 社で営業秘密漏えい防止策を導入。

	企業	導入済みもしくは導入が決まっている対策
1	B 社	・シュレッダーの増設 ・SNS や携帯電話の使用ルールの作成 ・管理ルールの改正 ・部外者立ち入りルールの作成
2	C 社	・就業規則の改正
3	E 社	・監視カメラの増設
4	J 社	・規定の改正
5	K 社	・機密保持契約書、労働契約書、就労規則の改正
6	O 社	・管理強化のためルール・雇用契約書等を作成
7	P 社	・一部の文書において閲覧制限を実施
8	R 社	・情報管理規程の作成

9	U 社	・秘密情報管理制度、管理ガイドラインの制定 ・定期的な秘密情報ヒヤリハットの事例紹介による意識強化

〔3〕普及啓発

1. 概観

営業秘密管理体制のモデルケースや流出事例、過去の支援利用企業の事例を紹介し、営業秘密管理の重要性について啓発するとともに、個別支援のニーズを掘り起こすことを目的として、企業関係者に対しセミナーを行った。

また、技術流出防止管理説明会（後掲4. 参照）に講師を派遣した。

2. 個別支援企業募集セミナー

専門家より営業秘密漏えい対策について講演を行い、前年度利用企業にも登壇いただくとともに、ジェトロ職員から営業秘密漏えい対策支援事業について紹介する WEB セミナーを日本国内（東京）及び中国（上海）で開催した。

（1）日本

- ・ 実施日時 2021 年 6 月 24 日（木）14：00～16：25
開催形式 WEB セミナー
参加人数 107 名

（2）中国

- ・ 実施日時 2021 年 7 月 1 日（木）14：30～16：10
開催形式 WEB セミナー
参加者数 103 名

3. 成果普及セミナー

欧米および韓国、それぞれの専門家より、営業秘密漏えい対策について講演を行う WEB セミナーを日本国内（東京）で開催した。

- ・ 実施日時 2022 年 2 月 17 日（木）10：00～12：00
開催形式 WEB セミナー
参加人数 172 名

4. 技術流出防止管理説明会

ジェトロ職員を派遣し、営業秘密保護及び技術流出防止のための対策について講演を事前収録し、技術流出防止管理説明会において当該講演動画の配信を行なった。

- ・ 実施日時 2021 年 6 月 4 日（金）、9 日（水）、18 日（金）、28 日（月）、7 月 5 日（月）、12 日（月）、16 日（金）、28 日（水）、8 月 2 日（月）、18 日（水）、30 日（月）、9 月 17 日（金）、28 日（火）、29 日（水）、10 月 15 日（金）、11 月 1 日（月）、24 日（水）、12 月 3 日（金）、17 日（金）、1 月 12 日（水）、2 月 9 日（水）、15 日（火）

2022 年 1 月 12 日（水）、2 月 9 日（水）、15 日（火）

開催形式 WEB セミナー

[4] マニュアル・調査レポート作成

1. 概観

シンガポール、韓国について、関係法令における営業秘密の定義・対象範囲（侵害行為）・法的措置（民事救済・刑事罰等）、営業秘密の流出事例、営業秘密の判例・紛争事例、営業秘密の保護・管理上で特に気を付けるべきポイント、参考となる資料（各種ひな形等）からなる営業秘密管理マニュアルを作成した。

また、米国、欧州（EU、ドイツ、イギリス）について、営業秘密の法制度調査を行った。（別紙参照）。

経済産業省委託事業

**シンガポールにおける
営業秘密管理マニュアル**

2022 年 3 月

**独立行政法人 日本貿易振興機構
シンガポール事務所
(知的財産部)**

報告書の利用についての注意・免責事項

本報告書は、日本貿易振興機構（ジェトロ）が現地調査会社に委託し作成したものであり、調査後の法律改正などによって情報が変わる場合があります。掲載した情報・コメントは調査委託先の判断によるものであり、情報の正確性や一般的な解釈がこのとおりであることを保証するものではありません。また、本報告書はあくまでも参考情報の提供を目的としており、法的助言を構成するものではなく、法的助言として依拠すべきものではありません。本報告書にてご提供する情報等に基づいて行為をされる場合には、必ず個別の事案に沿った具体的な法的助言を別途お求め下さい。

ジェトロおよび調査委託先は、本報告書の記載内容に関して生じた直接的、間接的、派生的、特別の、付随的、あるいは懲罰的な損害および利益の喪失について、それが契約、不法行為、無過失責任、あるいはその他の原因に基づき生じたかにかかわらず、一切の責任を負いません。これは、たとえジェトロまたは調査委託先が係る損害等の可能性を知らされていても同様とします。

JETRO - 営業秘密マニュアル

目次

I.	はじめに	5
II.	第1部:法制度.....	6
(1)	シンガポールにおける営業秘密の定義と範囲（シンガポールと日本の違い）	6
1.1	「営業秘密」の定義.....	6
1.2	営業秘密の保護の範囲	8
1.3	シンガポールと日本の違い.....	9
1.4	まとめ.....	11
(2)	営業秘密の管理方法.....	12
2.1	企業機密をどう管理・共有するか — 保護のための実務... ..	12
2.2	シンガポール国外への営業秘密の移転	13
2.3	登録要件	16
2.4	まとめ.....	16
(3)	営業秘密の侵害	17
3.1	秘密保持義務違反（BOC）	17
3.2	その他の、実務上可能な請求原因.....	20
3.3	まとめ.....	20
(4)	救済手段	21
4.1	民事上の救済手段	22
4.2	刑事上の制裁手段	25
4.3	裁判外の紛争処理	27
4.4	まとめ.....	29
(5)	統計情報	29
(6)	秘密の保護に関する法律の発展動向	29
6.1	BOC に関する伝統的なテストから離れ、「I-Admin」事件の判断要素へ	29

6.2	衡平法上の損害賠償の利用可能性.....	31
6.3	まとめ.....	32
III.	第2部：漏洩防止のための実務的な対策	33
(1)	シンガポールにおける秘密情報管理の手順	33
(2)	秘密情報に関する契約書作成上の留意事項	39
2.1	秘密保持条項.....	39
2.2	競業避止条項及び勧誘禁止条項	42
2.3	分離条項.....	43
2.4	準拠法及び裁判管轄条項	43
(3)	漏えい事案への対応.....	43
(4)	参考資料:関連文書等のフォーマット例	45
	附属書 A.....	46
	附属書 B.....	50
	附属書 C.....	53
	附属書 D.....	59
	附属書 E.....	61

I. はじめに

市場において、自社製品・サービスが競争力を発揮するためには、それらを支える自社独自の技術情報や営業情報といった営業秘密を適切に保護することは極めて重要であり、製造、販売等の拠点を海外にも有する場合には、各国における関連法規や権利行使のプラクティス、商習慣等の相違を考慮した上で、拠点ごとに営業秘密を適切に管理する必要がある。

とりわけ、シンガポールでは営業秘密が法令において定義されていないことから、ある情報が営業秘密であるかを判断するにあたって裁判例を考慮する必要がある。例えば、シンガポールでは、「営業秘密」に該当するために必要な要件は存在しないが、裁判所は、ある情報が「営業秘密」であるか否かを判断するに当たって、情報の性質、情報にアクセスすることを許可された者、及び当該情報を保護するために実施されている保護措置などを含む、多くの要因を考慮に入れることとしている。

そこで、本稿は、こうした実情を踏まえ、日系企業のシンガポールにおける営業秘密管理体制の整備・構築、又はその見直しに資するべく、シンガポールにおける営業秘密の管理方法について、現地専門家の経験を踏まえて、基本マニュアルとしてまとめたものである。

本稿は、「法制度編」と「漏えい対策実践編」から構成され、いずれのパートについても、日本との異同や日本との比較において、シンガポールで特に留意すべき点を中心に説明している。もっとも、シンガポールにおいて、営業秘密の不正取得からの保護、競合者による営業秘密の利用に対処するという点で、日本における営業秘密管理の考え方と共通する部分も多く、経済産業省の「秘密情報の保護ハンドブック～企業価値向上に向けて～」(以下、本稿では「ハンドブック」という。)の内容が参考になると考えられるため、本稿とあわせて活用することで、ぜひ、シンガポールにおける営業秘密の管理の整備にお役立て頂きたい。

II. 第1部:法制度

(1) シンガポールにおける営業秘密の定義と範囲（シンガポールと日本の違い）

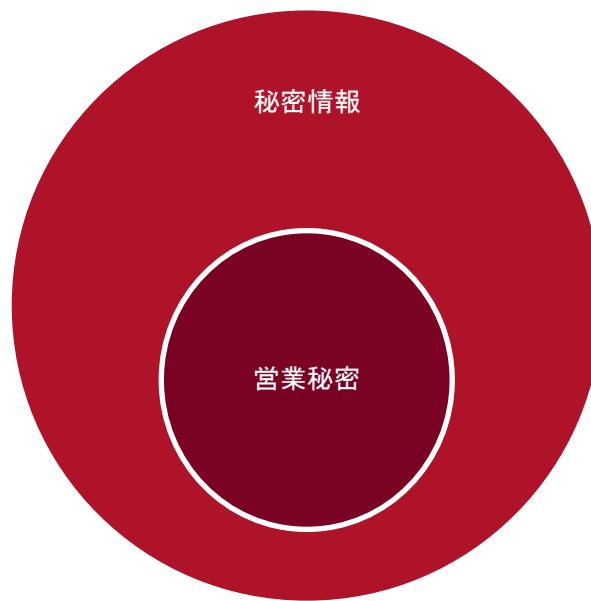
1.1 「営業秘密」の定義

シンガポールにおける営業秘密の保護について、同国はWTO（世界貿易機関）の加盟国であり、TRIPS協定（知的所有権の貿易関連側面に関する協定）において「開示されていない情報の保護」（同協定第39条）が加盟国の義務として定められていることから、日本と同様、企業・事業者等が保有する営業秘密について、法的な保護を受けることが可能である。

しかし、アメリカやイギリスなど判例法（コモンロー）が主たる法源となるシンガポールでは、日本の不正競争防止法のような営業秘密の保護を規定する明確な法律は存在せず、「営業秘密」という用語の法律上の定義も存在しない。「営業秘密」という用語は一般的に、高度に秘密であるか又は機微性の高い情報、例えば秘密の化学式や秘密の製造プロセスを指すものとされている¹。

シンガポールの裁判所では、営業秘密は、秘密情報の一形態であって、その中で最高度の秘密性を有するもの、としている。下の図は、秘密情報と営業秘密の関係を示したもので、営業秘密は秘密情報の一部に含まれるものとなっている。

¹ Ng-Loy Wee Loon, *Law of Intellectual Property in Singapore*（「Ng-Loy 論文」）, [38.0.1].



「秘密情報」についても、法令上の定義はない。「秘密情報」は、一般に「必要な程度の秘密性を有する情報」をいうとされている²。その意味するところは、当該情報がパブリックドメインの中で自由に利用可能な状態ではなく³、かつ、公有の財産又は公知の知識となっていないこと、である⁴。裁判所は、ある情報が秘密であるかの判断にあたって、過去の裁判所の判決を参照することができる。シンガポール及びその他のコモンローの国、例えば英国、カナダ、香港、そしてオーストラリアなどの裁判所の判決が公開されている。

営業秘密に関する裁判所の判決の内容又は記録の公開にあたっては、特段の制限はない。

従業員との関係では、特に退職した従業員について、「営業秘密」と、

² Ng-Loy 論文 [39.1.1].

³ *Stratech Systems Ltd v Guthrie Properties (S) Pte Ltd* [2001] SGHC 77 (「Stratech 事件」) at [37]。また、<https://www.ipos.gov.sg/about-ip/other-ips/confidential-information-trade-secrets> で閲覧可能 (2020 年 12 月 20 日時点) である、シンガポール知的財産局 (「IPOS」) の「*Confidential Information & Trade Secrets*」 (「IPOS - CI & TS」) も参照のこと。

⁴ *Stratech* 事件で高等裁判所の引用した、*Saltman Engineering Co Ltd v Campbell Engineering Co. Ltd* [1948] 65 RPC 203 at 215

営業秘密のレベルに達しない単なる「秘密情報」との区別が重要となることがある。

- 営業秘密については、雇用後に従業員であった者が当該営業秘密を開示又は使用しないことは、黙示的な義務となっている。黙示的な義務は、明示的な書面による義務がなかったとしても適用される。
- 対照的に、このような黙示的な義務は、単なる秘密情報については存在しない。退職者は通常、退職後の当該秘密情報の使用及び開示に関して、雇用契約における明示的な条件にのみ拘束される。

営業秘密又はこれと同等のものに具体的に何が該当するのかという網羅的なリストは存在しない。製造過程における秘密などは営業秘密の典型例であるが、この他、無数の多様な情報が営業秘密となりうる。もっとも、一部の情報については、それが秘密といえる期間は短いかもしれない。例えば、特許による保護を求めて企業自身が情報を公衆に開示することによって、当該情報が秘密性を失う場合などがある⁵。

最終的に、ある情報が営業秘密であるか否かを決定する際には、裁判所は、情報の性質、それにアクセスすることを許可された者の指定、流通の程度、及び自由に開示することができる他の情報から容易に分離することができるか否かを含め、様々な要素について検討を行う。これは、事案ごとの判断となる。秘密情報（4 ページを参照のこと）と同様に、ある情報が営業秘密であるかどうかの判断にあたっては、裁判所は過去の裁判例を参照することができる。

1.2 営業秘密の保護の範囲

シンガポールでは、秘密情報について出願・登録などの手続きはなく、また、秘密情報又は営業秘密が保護される期間についての法定の期間又は制限も存在しない。

一般的に、営業秘密は、コモンロー上の秘密侵害の原則（「**BOC: breach of confidence**」）、及び（該当する場合には）知的財産（「**IP : Intellectual Property**」）法及び契約法により保護される。秘密情報（営業秘密を含む。）を知り得た者は、一般に秘密を保持する義務を負

⁵ *Tang Siew Choy v Certact Pte Ltd* [1993] 1 SLR(R) 835 at [16].

い、第三者に開示することはできない。もし秘密情報を開示した場合、その者は、当該秘密情報の所有者に対して、BOCに基づく不法行為について責任を負うこととなる。

典型的には、秘密情報は、多くの手段を通じて保護される。例えば秘密保持契約（「**NDA: non-disclosure agreement**」）では、契約上、当事者の情報を秘密に保持すること、当該情報へのアクセスを制限すること、組織内で適切な手順を講じること、当該秘密情報と営業秘密の流布に関する明確な記録を保持することを要求する⁶。「当該秘密情報と営業秘密の流布に関する明確な記録を保持すること」とは、例えば、組織は、機密情報の開示先、開示日、開示された機密情報、及びそのような開示に付随し、関連する保護措置について記録しておくことなどである。

1.3 シンガポールと日本の違い

日本とシンガポールにおける「営業秘密」の定義の比較を、下の図に示す。

シンガポール	日本
・法令において定義されていない。 ・秘密情報の一形態である。 ・一般的には、高度に秘密又は機微性の高い情報を示す。 ・ある情報が営業秘密であるかを判断するにあたって、裁判所は多数の要素を考慮する。例えば、情報の性質、これにアクセスすることが許されている人物の指定の有無、情報の配布が許されている範囲、当該情報が他の自由に開示できる情報から容易に区別できるようになっているか、等である。	・不正競争防止法（不競法）において、「技術上又は営業上の情報」であって以下を満たすものとして明示的に定義されている。 ・ 保有者の事業活動に有用な価値ある情報であること ・ 秘密として保有または管理されていること ・ 公然と知られていないこと ・ただし、不競法は、上記の各要素についてのさらなる定義は定めていない。

日本の不正競争防止法（不競法）では、当該情報が秘密情報として管理されていることを立証するためには、営業秘密保有企業が当該情報を秘密であると単に主観的に認識しているだけでは不十分であり、営

⁶ IPOS - CI & TS

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⁷によって、従業員に明確に示され、結果として、従業員が当該秘密の保有者の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）必要がある。しかし、シンガポールとは異なり、一般的な「秘密情報」と比較して「営業秘密」が高度に秘密である、又は機微情報であることは要求されていない。

シンガポールのルールと日本の不競法とのもう一つの大きな違いは、不競法ではどのような行為が不競法違反（すなわち、営業秘密の侵害）を構成するかを規定していることである。その行為は、次のとおりである（括弧内は該当条文）。

- 窃盗、詐欺、強迫その他不正の手段により営業秘密を取得し、又は当該不正取得により取得した営業秘密を使用し、もしくは開示する行為（不競法第2条第1項第4号）
- その営業秘密について不正取得が行われたことを知って、又は重大な過失により知らないで営業秘密を取得し、使用し、もしくは開示する行為（不競法第2条第1項第5号）
- 当該営業秘密について不正取得があったことを知った後、又は、重大な過失により知らなかった場合に、取得した営業秘密を使用又は開示する行為（不競法第2条第1項第6号）
- 不正の利益を得る、又は保有者に危害を加える目的で保有者から示された営業秘密を使用し、又は開示する行為（不競法第2

⁷ 秘密管理性要件は、従来、①情報にアクセスできる者が制限されていること（アクセス制限）、②情報にアクセスした者に当該情報が営業秘密であることが認識できるようにされていること（認識可能性）の2つが判断の要素になると説明されてきた。しかしながら、両者は秘密管理性の有無を判断する重要なファクターであるが、それぞれ別個独立した要件ではなく、「アクセス制限」は、「認識可能性」を担保する一つ的手段であると考えられる。したがって、情報にアクセスした者が秘密であると認識できる（「認識可能性」を満たす）場合に、十分なアクセス制限がないことを根拠に秘密管理性が否定されることはない。もっとも、従業員等がある情報について秘密情報であると現実に認識していれば、営業秘密保有企業による秘密管理措置が全く必要ではないということではない。法の条文上「秘密として管理されている」と規定されていることを踏まえれば（法第2条第6項）、何らの秘密管理措置がなされていない場合には秘密管理性要件は満たさないと考えられる。

条第1項第7号)

- 上記の不正取得行為により営業秘密が開示されていることを知って、又は重大な過失により知らないで、営業秘密を取得し、使用し、又は開示する行為（不競法第2条第1項第8号）
- 不正取得行為により当該営業秘密が開示されたことを知った後、もしくは重大な過失により知らなかった場合に、当該営業秘密を使用し、又は開示する行為（不競法第2条第1項第9号）
- 技術上の営業秘密の前述の使用行為（不正使用行為）によって生じた物を譲渡、引き渡し、展示、輸入、輸出、又は電気通信回線を通じて提供する行為（不競法第2条第1項第10号）

さらに、シンガポールでは、単なる秘密情報と区別して別途営業秘密を定義し、営業秘密にのみ退職者が在職中の営業秘密を開示又は使用しないという黙示の義務が課される。一方で、日本の不競法はこのような構造を採用していない。

他方、日本における営業秘密の保護に関する法律の規定は、以下の点でシンガポールのルールと同一である。

- 営業秘密の出願・登録手続きは存在せず、営業秘密を保護することができる期間を規定した法定の期間又は制限も存在しない。
- また、特許法等の知的財産法、契約法、不法行為法の違反（該当する場合）の原則により、不競法上の営業秘密に該当しない情報を保護することも可能である。
- 日本でも、秘密保持契約（「NDA」という。）を通じて、契約上、当事者に保持している情報を秘密にすること、当該情報へのアクセスを制限すること、適切な手段を講じ、当該秘密情報・営業秘密の流出に関する明確な記録を保持することなどを要求することにより秘密情報を保護することが一般的である。

1.4 まとめ

- シンガポールにおいて、営業秘密は秘密情報の一形態である。
- シンガポールにおいて、「営業秘密」あるいは「秘密情報」についての法律上の定義はないが、判例法であるコモンローによ

り、「営業秘密」は秘密情報のうち高い程度の秘密性を有するものとされている。他方で「秘密情報」は一般に、パブリックドメインの中で自由に利用可能な状態ではない、必要な程度の秘密性を有する情報を指すものとされている。

- この点で、「営業秘密」について不競法による明示的な定義を置いている日本とは異なる。
- 営業秘密は一般的に、コモンロー上の法理である「BOC」、及び要件を満たす場合には知的財産法及び契約法において保護されている。

(2) 営業秘密の管理方法

2.1 企業機密をどう管理・共有するか ― 保護のための実務

1. 上記のとおり、シンガポールでは「営業秘密」は定義されておらず、情報の一部が「営業秘密」に該当するために必要な決まった要素は存在しない。しかしながら、裁判所は、ある情報が「営業秘密」であるか否かを判断するに当たって、情報の性質、情報にアクセスすることを許可された者、及び当該情報を保護するために実施されている保護措置などを含む、多くの要因を考慮に入れる。したがって、営業秘密を保有するすべての組織は、中小企業から国際的な企業に至るまで、その営業秘密を保護するための実効的な措置を講じるべきである。

企業の内部及び外部で（例えば、シンガポール法人と、現地パートナー企業及び委託先との間の関係において）営業秘密を管理するための4つの重要なステップは、次のとおりである：

- 企業等が保有する情報の中から営業秘密を特定すること。
- 企業の営業秘密のカタログ又はリストを作成し、どのような営業秘密を企業が保有し、当該営業秘密の秘密管理措置としてどのような保護手段が講じられているかを継続して確認・フォローできるように、随時更新すること。
- 営業秘密保護のための契約や、物理的及び技術的措置を組織全

体で講じること。

- 不正があった場合の行動計画を策定すること。

これらの施策は、社内で、またグループ会社における子会社間で横断的に適用されるべきである。もちろん、各社の正確な対応策や対応計画は、事業や業務の性質、営業秘密の性質、従業員の営業秘密へのアクセスの必要性、グループ会社間取引の性質などを考慮に入れて策定されるべきである。

4 つのステップの詳細と、営業秘密の漏洩防止のための具体的な対策については、第 2 部(1)「シンガポールにおける秘密情報の管理の方策」を参照されたい。III

2.2 シンガポール国外への営業秘密の移転

日本の不競法では、不正に取得した営業秘密（情報自体）の開示について不競法に違反すると定めているところ（不競法第 2 条第 1 項第 4 号～第 9 号）、開示先について国内向け・国内向けの区別はないことから、いずれも営業秘密の開示（移転）として不競法に違反することとなる。また、不正に入手した営業秘密の使用行為により生じた物を譲渡し、引き渡し、譲渡若しくは引渡しのために展示し、輸出し、輸入し、又は電磁的に提供する行為も不競法に違反すると定めている（不競法第 2 条第 1 項第 10 号）。

シンガポールでは、営業秘密をシンガポールから他国へ開示・移転することを規制する法律は存在しない。しかし、営業秘密の侵害により生じた物の譲渡、引き渡し、譲渡若しくは引渡しのための展示、輸出、輸入、又は電磁的提供行為については、下記の第 I 部(3)(3.1)で解説する BOC に基づく請求原因のための 3 要素を満たす場合には、侵害行為となりうる。

一般的に、企業としては、開示・移転される営業秘密を特定し、そのような営業秘密の開示・移転を保護するための措置を講じ、そのような措置が現場で適切に実施されることを確保すべきである。

さらに、当該営業秘密が 2012 年シンガポール個人データ保護法（「PDPA (Singapore Personal Data Protection Act 2012)」）に基づく

「個人データ」を構成する範囲において、組織⁸は、当該営業秘密が PDPA 第 26 条に基づく「**移転制限義務**」を遵守することを確認しなければならない。これにより、シンガポール国外の国又は地域への個人データの移転は、移転された個人データに付与される保護の基準が PDPA に基づき提供される保護と同等であることを確実にする、という法の要件に従う場合を除き、禁止されている⁹。

この点は、例えば、当該営業秘密に PDPA の下で「個人データ」とみなされる顧客リスト及び情報が含まれる場合などに関係する可能性がある。

移転制限義務の内容に関して、2014 年個人データ保護規則（**Personal Data Protection Regulations 2014**。「**本規則**」）は、組織が個人データをシンガポール国外の国又は地域に移転する前に、次のことをしなければならないと規定している。

- 移転された個人データに関して PDPA の他のすべての条項に確実に準拠するために適切な措置を講じること
- 移転された個人データの受領者が、移転された個人データに少なくとも PDPA の保護と同等の保護基準を提供するという法的強制力のある義務に拘束されることを確保するために、適切な措置を講じること

法的強制力のある義務は、2 つの方法で受領者に対して課すことが可能である¹⁰。

⁸ PDPA に基づき、「組織」とは、(a)シンガポールの法律に基づき設立されたか承認されたか否かを問わず、または(b)シンガポールに居住するか、または事務所もしくは事業所を有するか否かを問わず、業務であるか非業務であるかを問わず、あらゆる個人、会社、団体または個人の団体を含む。第 2 条参照。

⁹ PDPA 第 2 条は、「個人データ」を、「個人に関するデータであって、当該データから、又は当該データと組織が実際にアクセス又はアクセスする可能性のあるその他の情報から当該個人を識別することができるもので、真実であるか否かを問わない」と定義している。

¹⁰ シンガポール個人情報保護委員会（「PDPC」）、特定のトピックスに関する個人情報保護法に関する諮問指針（*Advisory Guidelines on the Personal Data Protection Act for Selected Topics*）（2020 年 6 月 2 日改訂）（「主要概念に関する指針」）（[https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-\(2-June-2020\).pdf?la=en](https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-(2-June-2020).pdf?la=en)）、19.3 項及び 19.4 項参照）。

- 第 1 に、以下のいずれかの形態で受領者に課す場合。
 - (i) 法律（規則を含むがこれに限定されない。）
 - (ii) 個人データを移転することができる国及び地域を限定した契約
 - (iii) 拘束力のある会社規則¹¹であって、当該拘束力のある会社規則が適用される移転個人データの受領者、当該個人データが移転される国及び地域、並びに拘束力のある会社規則により課されるそれぞれの権利及び義務を定めているもの
 - (iv) その他の、法的拘束力のある証書¹²
- 第 2 に、個人データが転送される国又は地域の法律に基づき付与又は承認された「特定認証（specified certification）」を受領する主体が保有している場合。なお、「特定認証」とは、アジア太平洋経済協力 越境プライバシー規則（「APEC CBPR」）システム又はアジア太平洋経済協力 プライバシー処理者認定（「APEC PRP」）システムに基づく認証を意味する。これは、シンガポールと日本の両国が APEC CBPR システムに参加していることに関連している。PDPA が受領する主体に課す移転制限義務は、以下の場合に満たされる。
 - (i) 受領者が組織として個人データを受領し、有効な APEC CBPR システムの認証を保有している場合
 - (ii) 受領者が、個人データをデータ仲介者¹³として受領し、

¹¹ このような拘束力のある会社規則は、受領者が移転する側の組織に関連する組織であり、まだ移転に関連する他の法的強制力のある義務（規則に定められているもの）をまだ受けていない場合に、採択することができる。さらに、規則では、次の場合、受領者が「移転する側の組織に関連している」と規定している。すなわち、(a) 受領者が、直接・間接を問わず、移転する側の組織を支配している場合 (b) 受領者が、直接・間接を問わず、移転する側の組織によって支配されている場合 (c) 受領者と移転組織が、直接・間接を問わず、共通の者の支配下にある場合、である。

¹² 主要概念に関する指針、第 19 章

¹³ PDPA の下では、「データ仲介業者」とは、他の組織に代わって個人データを処理する組織を意味するが、他の組織の従業員は含まない。第 2 章参照。また、「処理」とは、個人データに関連して業務又は一連の業務を遂行することを意味し、記録、

有効な APEC CBPR 又は PRP システムの認証のいずれか、又はその両方を保有している場合

さらに、事業者が提供するクラウドサービスを使用して個人データがシンガポール国外に転送される場合、当該サービスを利用する企業は、当該事業者が、(a)同等のデータ保護体制を有する場所にのみデータを転送すること、又は(b)移転されたデータについて同程度の保護基準を保証する法的強制力のある義務を負うこと、を保証しなければならない。これは、クラウドサービス提供事業者との適切な条件による契約を通じて行うことが可能である¹⁴。

たとえば、ある組織 ABC が、グループの集中的な顧客管理システムを通じて、顧客の個人データを海外の親会社に移転しているとする。移転される個人データに適用される保護の規定を含む移転の条件は、組織 ABC とその本社の双方に適用される拘束力のある会社規則に定められている。組織 ABC は、これらの拘束力のある会社規則を検討し、それらが規則に基づいて定められた条件を満たしており、PDPA に基づく基準と同等の保護を提供するものであると評価した。この場合、組織 ABC の海外への個人データの譲渡は、譲渡制限義務を遵守したものとされる¹⁵。

営業秘密の漏洩防止のための具体的な対策については、第 2 部を参照のこと。III

2.3 登録要件

シンガポールには営業秘密保護の登録要件は存在しない。

2.4 まとめ

- 企業は、保有する営業秘密を特定しリスト化するためのシステムを導入し、営業秘密を保護するための契約上、物理的、技術

¹⁴ 保管、整理、改変、検索、組合せ、送信及び消去又は破棄を含む。第 2 章参照。
個人データ保護委員会の「特定のトピックスに関する個人情報保護法に関する諮問指針 (Advisory Guidelines on the Personal Data Protection Act for Selected Topics)」(2019 年 10 月 9 日改訂)。<https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Selected-Topics/Advisory-Guidelines-on-PDPA-for-Selected-Topics-9-Oct-2019.pdf?la=en> で閲覧可能 (2020 年 12 月 20 日時点) である。

¹⁵ 主要概念に関するガイドライン、19.6 項。

的、組織的な保護措置を導入し、不適切な取り扱いがあった場合のアクションプランを策定すべきである。

- 営業秘密をシンガポール国外に開示・移転すること自体を規制する法律は存在しない。しかし、企業は、当該開示・移転が関連の法律を遵守したものであることの確認をする必要がある。
- シンガポールでは、営業秘密を保護するにあたって営業秘密を登録することは必要とされていないし、またそのための制度も存在しない。

(3) 営業秘密の侵害

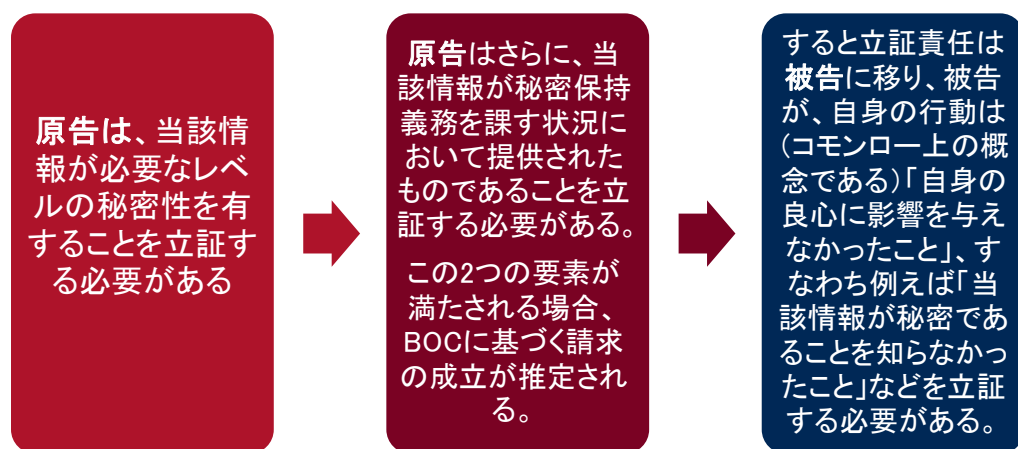
上記のように、営業秘密は、一般的に **BOC** に関するコモンローの原則、知的財産法、そして契約法などによって保護されている。以下、各概念について説明する。

3.1 秘密保持義務違反 (BOC)

秘密情報（営業秘密を含む。）にアクセスできる者は、一般に秘密を保持する義務を負い、第三者に開示することはできない。当該情報を開示する者は、当該秘密情報の所有者に対し、**BOC** に基づく不法行為について責任を負う。

BOC に基づく訴訟は、以下のステップで行われる¹⁶。

¹⁶ *I-Admin (Singapore) Pte Ltd v Hong Ying Ting and others* [2020] 1 SLR 1130 (「*I-Admin 事件*」の [61])。



(A) 当該情報は、秘密でなければならない

必要な程度の秘密性を有する情報とは、公衆が自由に入手できない情報をいう¹⁷。現段階では、営業秘密に関する企業内の方針及び保護措置が取られていることをもって、営業秘密が公衆の利用に供されていないことを証明することを助けることができる¹⁸。

(B) 情報は、秘密保持義務を課す状況において提供されなければならない

BOC に基づく請求の第 2 の要素は、営業秘密の所有者・占有者と受領者との間に明示的に（例えば、雇用契約又は秘密保持契約の中の秘密保持条項を通じて）又は黙示的に、当該営業秘密に関して秘密を保持する義務を課す契約が存在する場合に満たされる¹⁹。

そのような明示的又は黙示的な契約上の義務がない場合でも（すなわち、法的義務がない場合であっても）、当事者は、依然として、営業秘密を守る衡平法上の義務を負う場合がある。つまり、当事者間で秘密保持義務を定めた契約がない場合でも、秘密情報を受け取った当事者に、そのような情報を秘密にすることを義務付ける衡平法上の義務を

¹⁷ *Stratech* 事件の[33]

¹⁸ *Clearlab SG Pte Ltd v Ting Chong Chai* [2015] 1 SLR 163（「*Clearlab* 事件」）の[135]を参照。

¹⁹ *Clearlab* 事件の[65]を参照。

課することができる。営業秘密が開示された状況が、合理的な人物がその状況を考慮すれば、当該情報が当事者にとって秘密であることを認識できるような状況であることについて、当事者が証明することができる場合に衡平法上の義務が生じ、従って受領当事者に衡平法上の守秘義務が課されることになる。

この段階において、営業秘密、企業内の慣行、従業員に与えられた営業秘密へのアクセス権の程度、及び営業秘密の管理及び保護の方法に関する企業の規定類及び保護措置の存在は、当該秘密が秘密保持義務が課された状況下で開示されたことを証明するのに有用である。

(C) 被告による、(コモンロー上の概念である)「良心が影響されなかったこと」の証明

上記 2 つの要素が満たされた時点で、BOC に基づいた請求の成立が推定されるため、被告が、これに対する反証をしなければならない。例えば、以下のような事情の存在の証明である。

- 営業秘密が、必要な程度の秘密性を有していなかったこと、又は秘密保持義務を課す状況において付与されなかったこと。例えば、当該営業秘密について、当該企業の従業員が自由に営業秘密にアクセスし、そして公知となったことや、当該営業秘密が既に公知となっていたことを証明できる場合がある。
- コモンロー上の概念である「良心が影響を受けなかった」こと。これは例えば以下のようなものである。

(iii) 情報の秘密性を知らなかった場合（意図的に知らないようにした場合の判断や、被告側の過失が本要件の判断に影響するのといった点については、議論の余地がある。）

(iv) 偶然その情報に触れた場合

(v) 当該情報が、公衆の利用に供された物、又は取得者が合法的に所有していた物から、独立の創作又は独立の研究・リバーズエンジニアリングを通じて取得された場合

(vi) 公衆の利益に関するものであって、公にされるべき情報である場合（例えば、情報が何らかの不正に関する情報

である場合)。この抗弁は、警察等の、情報を受領する適切な利害関係を有する者に対する開示のみが対象である。

3.2 その他の、実務上可能な請求原因

(A) 著作権法

著作物（例えば、取扱説明書、コンピュータソフトウェア、データベースなど）から構成される営業秘密は、秘密情報に関する法の規定に加え、著作権法によって保護される²⁰。

例えば、コンピュータソフトウェア開発者は、基盤となるソフトウェアアーキテクチャ、アルゴリズム、ソースコードの著作権者として、それらの機密性を保ちつつ、自らのソフトウェアを商業化することができる。

したがって、著作物である営業秘密の所有者は、当該著作物を侵害した者に対し、著作権侵害に基づく救済を求めることができる。これらには民事上の救済措置及び刑事上の制裁措置も含まれる（下記第1部(4)4.2を参照）。

II3.24.2

(B) 契約違反

営業秘密の所有者と侵害者との間に当該営業秘密を保護する契約がある場合は、侵害者は契約違反という点に対しても責任を負う可能性がある。これは、両当事者間の契約条件及び両当事者の関係によることになる。

(C) 時効について

BOC、著作権侵害、契約違反に基づく訴えの時効期間は、請求原因の発生した日から6年間となっている。

3.3 まとめ

- 営業秘密は、まず BOC の法理によって保護される。
- 営業秘密の不正な使用が著作権の侵害にも該当する場合、損害

²⁰ なお、一般原則として、秘密情報に関して特許による保護を求めることはできない。特許を取得した場合は他者が当該発明を使用する行為を排除する 20 年間の独占的な権利が付与されるが、代わりに、特許の出願の過程で発明を公開しなければならない。従って、当該情報はパブリックドメインとなり、秘密とは言えなくなるからである。

を受けた当事者は侵害者に対して、著作権侵害に基づく訴えを起こすことができる。

- 営業秘密の所有者と侵害者との間に当該営業秘密を保護することを内容とした契約が存在する場合は、侵害者は契約違反の責任も負うことになる。

(4) 救済手段

シンガポールにおいては、下記のような、日本の不競法において認められている秘密性の立証のための立証手段又は証拠収集手段が用意されているわけではない。

- 技術上の秘密を取得した者の当該技術上の秘密を使用する行為等の推定（不競法第 5 条の 2）
- 損害の額の推定等（不競法第 5 条）
- 秘密保持命令（不競法第 10 条）
- 当事者尋問等の公開停止（不競法第 13 条）

日本の法制度では、裁判所が当事者及び代理人に対して、審理中に提出された情報を第三者に対して公開することを禁じる秘密保持命令（不競法第 10 条）を出すことができる。この秘密保持命令違反に対しては、刑事罰も用意されている（不競法第 21 条第 2 項第 6 号）。

一方、シンガポールの裁判所でも、当事者が裁判所に対し、BOC の訴えにおける秘密情報を保護するための措置の申し出を行うことが可能である。例えば、第三者への開示を防ぐために、書面を名前で特定された「秘密のグループ」に対してのみ書面を公開することや、裁判ファイルに第三者がアクセスすることを禁止する封入命令、審理手続が非公開の法廷でのみ行われることを申し入れることが可能である。下の表は、シンガポールにおいて、営業秘密の侵害に対して認められている民事上及び刑事上の救済手段の概要を示したものである。

民事上の救済	刑事上の制裁
・ 中間的差止命令 ・ 搜索差押命令(アントン・ピラー命令) ・ キア・ティメット差止命令 ・ 損害賠償 ・ 永続的な差止命令 ・ 裁判所の引渡命令又は廃棄命令	・ 著作権法違反での訴追 ・ コンピューター不正使用法での訴追

4.1 民事上の救済手段

(A) 暫定的な救済

(i) 仮処分命令

BOC の状況では、被害を受けた秘密情報又は営業秘密の所有者・占有者は、裁判や仲裁の結果又はその他の事項の最終決定が出るまで、侵害者がその秘密情報・営業秘密を使用、悪用、開示、複製又はその他の方法で取り扱うことを防止するために、暫定的又は仮の差止命令を取得することを試みることができる。すなわち、シンガポールの裁判所は、当事者が秘密情報・営業秘密を第三者に開示することを、事件の審理の時まで禁止する命令を出すことが可能となっている。シンガポール裁判所規則 (Singapore Rules of Court) の Order 29 が、裁判所に、仮処分命令の権限を与えている。

暫定的差止命令を認めるべきか否かを検討するに当たり、裁判所は、次のことについて確証を得なければならない。

- 審理されるべき、深刻な問題があること (すなわち、その主張が法律上取り上げる価値がないもの、又は訴権の乱用的なものではないこと)。
- 差止命令が発せられない場合、損害賠償という手段では、請求人に加えられる可能性のある損害に対する適切な救済とはなら

ないこと。

- 比較衡量の結果、差止命令を認めることが好ましいと認められること。

(ii) アントン・ピラー (Anton Piller) 命令

申立人はまた、侵害者に対する訴訟において証拠を形成する書類その他の物件の調査、検査、除去又は写しを作成するために、侵害者の施設に立ち入るための搜索及び差押命令を裁判所に申請することができる。シンガポール裁判所規則 (Singapore Rules of Court) の Order 29 は、裁判所に対して、事件の対象物であるいかなる財物についても、その留置、管理又は保全の命令の実施の目的で、事件の当事者の占有する不動産に立ち入ることをいかなる者に対しても許可することのできる権限を与えている。

被告が当該書類又は物品を隠匿、破棄又は処分することを防止するために、当該申請は、(侵害者に通知することなく) 一方当事者のみの手続きで行われる。そのため、裁判所は、申立人による完全かつ率直な開示を要求し、そうでない場合には認められた命令は、取り消されることがある。申請者はまた、損害賠償・補償 (当該命令の実行によって生じた損失を被告に補償するためのもの) に関する誓約を行わなければならない。

搜索差押命令を確保するためには、申請者は、次のことを裁判官に納得させなければならない。

- 事実に基づき、違反についての極めて強い (すなわち、侵害者に対する請求・申立てが正当化される可能性が高い) 事例であること。
- 命令が出されない場合、請求する者に対する損害 (実際のもの又は潜在的なもの) が非常に大きいこと。
- 侵害者が証拠を破棄する可能性があること。
- 搜索差押の効果が、その正当な目的に見合ったものであること。

この救済手段は、秘密情報が保管されていると疑われる施設に入り、文書、記録、コンピューターデバイス (個人用も含む)、その他秘密情報が保管されていると思われるあらゆる媒体を押収し、当該保管媒体

を調査・検査し、及び/又は侵害者が所持するすべての秘密情報のコピーを除去することができるという、その侵襲的性質から裁判所に認められることは稀である。

(iii) キア・ティメット (Quia Timet) 差止命令

侵害が発生していないが、そのおそれがある又は差し迫っている場合は、営業秘密の所有者は、その発生前に営業秘密の開示を防止するために、キア・ティメット (Quia Timet) 差止命令を求める権利を有する²¹。

これは、被申立人による違反又は法律上の不正であって、そのおそれ又は差し迫った状況があり、かつ、それが回復することができない損害を請求人に与えるものである場合に、その実行を抑制するための差し止め命令である。

裁判所が当該差止命令を発する前に、請求人は、被申立人が請求人に回復不能の損害をもたらすような行為上の不正を犯す現実の危険があることを証明しなければならない。「回復不能の損害」とは、直ちに中間的差止命令を得ても回復することができず、かつ、請求人が損害賠償の判決を得ても十分に補償することができない損害をいう²²。

(B) 恒久的救済

契約違反及び秘密侵害の訴えの根拠は、制定法には存在しない。例えば契約違反・秘密侵害の訴えがシンガポール高等裁判所に提起されたとする。裁判所は、最高裁判所法において付与されている権限を行使できるとされており、最高裁判所法の第一別紙には、裁判所の権限には、「法及び衡平法上の全ての救助及び救済を与えることが含まれ、これには、差止命令又は特定履行に加え、又はこれに代わるものとしての、損害賠償を認めることが含まれる」と規定されている。これが裁判による救済の根拠となっている。

契約違反・秘密保持違反の訴訟に基づいて利用可能な民事救済は、以

²¹ *CDL Hotels International Ltd v Pontiac Marina Pte Ltd* [1998] 1 SLR(R) 975 において、シンガポール控訴裁判所は、キア・ティメット (quia timet) の申し立てを、「認識されている不正を避けるために提起される措置」と説明している。

²² *Royal Insurance Co Ltd v Midland Insurance Co.* (1908) 26 RPC 95 at [97]。これは、*Millennium Pharmaceuticals, Inc. v Drug Houses of Australia Pte Ltd* [2018] SGHC 149 at [88]で支持された。

下の通りである

- 損害賠償（補償としての賠償と秘密侵害に対する衡平法上の損害賠償を含む。）又は不当利得（I-Admin[56]を参照。）。なお、シンガポール法においては、契約違反には懲罰的損害賠償の判決を与えることはできないとの一般原則がある。シンガポール控訴裁判所はこの点に関する可能性を完全に否定してはいないものの、その可能性は「確かに、きわめてまれであろう」としている（Turf Club Auto Emporium Pte Ltd v Yeo Boong Hua [2018] 2 SLR 655 at [198]を参照のこと）。よって、秘密保持義務違反の損害賠償は、損害賠償（補償としての賠償と衡平法上の損害賠償を含む）及び不当利得に限定されている。
- 恒久的差止命令（例えば、侵害者が営業秘密を使用、悪用、開示、複製、又は他の方法で取り扱うことを制限するもの）（I-Admin[56]を参照。）
- 営業秘密の引渡し又は廃棄を命ずる裁判所の命令（I-Admin[56]を参照。）
- 著作権侵害訴訟において、裁判所は、著作権者に対し、将来の侵害を制限する差止命令、損害賠償もしくは不当利得又は法定損害賠償、及び侵害物品の引渡し・処分命令を言い渡すことができる。

4.2 刑事上の制裁手段

BOC に基づく訴えの対象となる行為は、シンガポールの他の法律に基づく違法行為に該当し、別途、刑事責任を生じさせることもある。なお、シンガポールにおいて、この刑事訴追には時効が存在しない。

(A) 著作権法

- 著作権法（2021年改正）第444条は、著作権が成立している著作物について、販売又は賃貸、商業的取引、商業的取引目的での輸入、又は商業的取引目的での保有を行うことは、当該物が著作物を侵害する複製物であることを知っていた（又は、知っているべき合理的理由があった）場合には、犯罪となると定めている。
- 著作権法（2021年改正）第445条は、商業的な利益を得る目的で権利の侵害を故意に行った者は罰する旨を定めている。

第 444 条に違反の行為を行った場合、個人であれば、100,000 シンガポールドル又は侵害の対象となった著作物ごとに 10,000 シンガポールドルの、いずれか高い方の金額を上限とした罰金、5 年以下の懲役、又はその両方が科される。法人の場合は、200,000 シンガポールドル又は侵害の対象となった著作物ごとに 20,000 シンガポールドルの、いずれか高い方の金額を上限とした罰金が科される。

第 444 条違反の行為を行った場合、個人であれば、100,000 シンガポールドルを上限とした罰金、5 年以下の懲役、又はその両方が科される。法人の場合は、200,000 シンガポールドルを上限とした罰金が科される。

(B) コンピュータ不正使用法

BOC の事案がコンピュータ内のデータ又はプログラムの不正なアクセス・改ざん（例えば、営業秘密を含む文書の電子的コピーの不正なダウンロード）を含む場合、これはシンガポールコンピュータ不正使用法(Cap. 50A)(「**CMA**」)に基づく違反も構成することがある。

CMA の違反は、その性質上、刑法犯である。被害者は、刑事告訴により、CMA 違反を警察に報告し、刑事訴追を求めることができる。CMC は、犯罪者、コンピュータ、プログラム又はデータが犯罪時にシンガポールに所在していた場合にのみ適用される。

CMA 第 3 条では、コンピュータに保存されているデータ又は又はプログラムへの不正アクセスを行う目的で、コンピュータ上で意図的に何らかの機能を実行させることが禁止されている。違法行為の成立のためには、当該資料が秘密の性質を有している必要はない。この不正アクセスには、従業員等が業務範囲外の目的のためにコンピュータファイルにアクセスする状況も含まれる。

第 3 条違反の罪で有罪となった者は、最初の違法行為については 5,000 シンガポールドル以下の罰金もしくは 2 年以下の懲役、2 回目及びその後の違法行為については 10,000 シンガポールドル以下の罰金、3 年以下の懲役、又はその両方が科せられる。不正アクセスの結果、損害が発生した場合には、非常に厳しい罰則が課される²³。

²³

CMA 第 3 項(1)及び(2)。第 3 条の違反の結果として損害が生じた場合、違反者には 50,000 ドル以下の罰金もしくは 7 年以下の懲役が科され、又はこれらが併科さ

CMA 第 5 条では、コンピュータの内容の不正な変更を引き起こすと知っている行為を行うことが禁止されている。第 3 条に基づいて有罪となった者には、最初の違法行為については 10,000 シンガポールドル以下の罰金、3 年以下の懲役、又はその両方、2 回目及びその後の違法行為については 20,000 シンガポールドル以下の罰金、5 年以下の懲役、又はその両方が科せられる。不正アクセスの結果、損害が発生した場合には、非常に厳しい罰則が課される²⁴。

さらに、CMA 第 13 条で、裁判所は、CMA に基づく犯罪で有罪判決を受けた者に対し、当該犯罪によりコンピュータ、プログラム又はデータに生じたいかなる損害についても、いかなる人物に対しても金銭的補償を行うよう命じることができる。当該補償金の支払命令は、当該命令に基づいて支払われた金額を超えて民事訴訟において損害賠償を請求する権利を妨げるものではない。原告は、そのような損害が発生した場合直ちに暫定的差止命令を得ても回復することができず、かつ、請求人が損害賠償の判決を得ても十分は補償を得られないことを証明する必要がある。

4.3 裁判外の紛争処理

当事者は、訴訟又は仲裁による訴訟手続の開始とは別に、調停等の裁判外の紛争解決手続による紛争の解決を検討することができる。

調停は、任意のプロセスである。調停の手続きでは、すべての関係当事者の同意に基づき、紛争当事者が紛争を友好的に内部で解決するのを助ける中立的な第三者の調停人が関与する。調停の内容は厳密に秘密性が保たれ、対立的な状況を避ける方法で行われる。調停は、多くの場合、当事者間の紛争を解決するのに時間と費用効率の良い解決方法であると考えられている²⁵。

当事者は、内部的に又は第三者機関が管理する調停の手続きで調停を

れる。

²⁴ CMA 第 5 条(1)及び(2)。第 3 条の違反の結果として損害が生じた場合、違反者には 50,000 ドル以下の罰金もしくは 7 年以下の懲役が科され、又はこれらが併科される。

²⁵ 2017 年 11 月 1 日、シンガポールにおいて調停法 (the Mediation Act) が運用開始された。この法律では、調停手続きにおける多くの法的な観点について明確化及び成文化がなされた。この法律は、シンガポールにおいて一部または全部の手続きがなされる調停、及び、当事者がシンガポール方を適用することに同意した調停に適用される。

行うことについて合意することができる。シンガポールでは、シンガポール調停センター（「SMC」(Singapore Mediation Centre)）とシンガポール国際調停センター（「SIMC」(Singapore International Mediation Centre)）が主要な機関となっている。

特に、2020年9月12日、SIMCと日本国際調停センター（「JIMC」）は、新型コロナウイルスのパンデミックの状況において、シンガポール・日本帯の企業を含むクロスボーダーのビジネス事業者に対し、商業上の紛争を解決するための経済的で、迅速かつ効果的なルートを提供するための共同プロトコル（「本プロトコル」）を運営するための覚書に署名した²⁶。本プロトコルは、あらゆる種類の国境を越えた紛争が、迅速、経済的かつ効果的な調停手続を通じて解決されることを可能にすることを目的としている。本プロトコルは2021年9月11日まで有効であった。

本プロトコルの主な特徴は次のとおりである²⁷。

- 調停は、JIMC 又は SIMC の何れかに、20,000 円又は 250 シンガポールドルのいずれか低い額を手数料として納付することにより、提出することができる。JIMC と SIMC は、調停を共同で管理する。
- 各事案は、経験豊富な 2 名の調停員（各機関が 1 名ずつ指名）によって解決される。
- 両当事者は、日本市場に適合した固定料金と割引料金という利益を享受できる。例えば、130 万シンガポールドル未満の紛争では、各当事者が支払うのは 6,500 シンガポールドルである²⁸。
- 調停は、現在の渡航に関する制限を回避するために、オンラインで実施することができる。

²⁶ http://simc.com.sg/v2/wp-content/uploads/2020/09/JIMC-SIMC-Joint-Protocol_FINAL-for-web.pdf でアクセスできる（2020年12月20日時点）。

²⁷ SIMC の、「JIMC - SIMC Joint COVID-19 Protocol」。 <https://simc.com.sg/jimc-simc-joint-covid-19-protocol/#:~:text=This%20is%20the%20first%20known,jurisdictional%20barriers%20to%20promote%20settlement> でアクセスできる（2020年12月20日時点）。

²⁸ http://simc.com.sg/v2/wp-content/uploads/2020/09/JIMC-SIMC-Joint-Protocol_FINAL-for-web.pdf で入手可能な料金表を参照のこと。

- 和解の合意書は、シンガポールをはじめとした、調停に関するシンガポール条約の批准国において、当該条約に基づいて執行することができる。

4.4 まとめ

- 営業秘密の不正使用をされた場合、民事及び刑事上の責任追及手段が用意されている。
- 民事責任に関しては、中間的差止命令や搜索差押命令といった仮の救済手段と、営業秘密の使用又は開示に対する恒久的な差止などの恒久的な救済手段、損害賠償、秘密情報の引き渡し又は廃棄といった救済手段が用意されている。
- 侵害者は、事案に応じて、著作権法・コンピュータ不正使用法などの刑事責任も負う場合がある。

(5) 統計情報

2015 年から 2019 年までの刑事事件及び民事事件の訴訟件数や、シンガポールにおける法的事件に関する勝訴数、敗訴数といった、公的に利用可能な統計的な情報は、存在しない。かかる統計情報は一般的に裁判所からは公開されていない。

近年の、BOC の法理に関する最も影響力の大きな判決は、「I-Admin」事件である。その概要は、下記の第 1 部(6)に記載の通りである。

(6) 秘密の保護に関する法律の発展動向

6.1 BOC に関する伝統的なテストから離れ、「I-Admin」事件の判断要素へ

伝統的に、秘密保持義務違反の請求は、次の 3 つの要素が示されることに基づいていた。すなわち、(a)当該情報がその性質上秘密であること、(b)秘密といえる状況において提供されたこと、及び(c)その情報が許可なく、原告に損害を与える形で使用されたこと、である²⁹。

しかし、デジタル化された社会を背景として、保護された情報（営業秘密を含む）の不正な複製、悪用、及び搾取を防止することは、今や

²⁹ I-Admin 事件の[43]。

著しく困難になっていることが認識されており、これに基づきシンガポール控訴裁判所は、最近、BOC クレームの判断基準を、上記の「I-Admin」事件で示された判断要素に変更した³⁰。

I-Admin 事件において、原告である I-Admin (Singapore) Pte Ltd. (「I-Admin (SG)」)は、給与管理データ処理サービス及び人事情報システムの事業を行っていた。同社は I-Admin (Shanghai) Ltd.をはじめとする多くの 100%子会社を運営していた。この事件の第一被告及び第二被告は、I-Admin (SG)及び I-Admin (Shanghai) Ltd.の元従業員であった。彼らは、I-Admin からの退職後、シンガポールに Nice Payroll Pte Ltd.という会社を設立し、同様に給与アウトソーシングサービスや人事管理機能を提供していた。Nice Payroll Pte Ltd.はこの訴訟の第三被告となっている。原告は、被告らの活動についてフォレンジック調査を行い、Nice Payroll の施設において搜索及び差押えを行うための裁判所からの命令を得た。これらの調査を通じて、原告は、被告の機器・サーバーから原告の資料を多数回収し、被告が電子メールでこれらの資料の一部を配布していることを発見した。これらの資料には、I-Admin (SG)のソースコード、給与システム及び人事サービスをサポートするデータベース、事業開発及び顧客関連資料、並びにその運営に関連する資料が含まれていた。原告はそこで、被告らに対し、秘密保持義務違反等を主張する訴訟を開始した。

伝統的な判断基準からの主な違いは、原告に損害を与える形で被告が秘密情報を不正に使用したことを立証しなければならないという原告への要件を撤廃することである。原告が、I-Admin 要素の最初の2つを証明した場合、(コモンロー上の概念である)「自己の良心への影響がなかったこと」を示すという立証の責任は被告に移ることになる。

このような立証責任の転換は、違反の可能性は数年後になって初めて発見される場合もあり、このため原告となる可能性のある者が、立証の観点から委縮してしまうという、秘密情報の所有者が直面する実際的な困難に対処しようとするものである。対照的に、I-Admin 事件における BOC の新たなテストは、被告人は請求の対象となる不正行為についての責任という点で、はるかに適切な位置にあるとの認識に立って

³⁰

I-Admin 事件の[3]。

いる³¹。

この **BOC** に基づく請求の法的枠組みの改正は、秘密情報を悪用した従業員に対峙する企業に対して、より大きな保護を与えることになる、歓迎すべき変更といえる。これは、企業が秘密情報の不正使用を立証する際の立証上の困難を解決するのに役立つといえる。今や、秘密情報にアクセスしたという行為それだけでも、請求を行うために十分なものとなっている。このことは、不正を行った社員が自分の痕跡を隠そうとするための措置を講じた場合に、特に役立つといえる。

6.2 衡平法上の損害賠償の利用可能性

さらに、**I-Admin** 事件の裁判所は、衡平法上の損害賠償が **BOC** の訴訟において利用可能な救済であることを明確にした。「衡平法上の損害賠償」とは、裁判所が損害賠償の額を査定するにあたって特定の根拠に限定されないという損害賠償である³²。これにより、裁判所は、損害賠償額の算定においてより柔軟性を持つことができるようになる。裁判所は、特定の要素又は枠組みに限定されることなく、損害賠償額の算定に最も適切であると考える方法を決定する裁量を持つ。

例えば、**I-Admin** 事件では、2 名の元従業員が原告の秘密情報（ソフトウェアやビジネス資料など）を悪用し、これを使って競合する事業を立ち上げ、それによって、当該資料や情報を開発する時間と手間を節約したという事情があった。原告に与えられる衡平法上の損害賠償の額の決定にあたって、裁判所は、下記の検討がこれに関連すると述べた³³。

- 被告が、もし原告の資料に接することなく当該ソフトウェア又は資料を作成しようとした場合に被告が出費したであろう追加費用
- 競業する事業を立ち上げ、それがより早く収益を上げられるようにできた時間の短縮

BOC に基づく案件において、衡平法上の損害賠償が利用可能になるというのは、それぞれの事件の状況において、最も適切かつ公正な救済

³¹ *I-Admin* 事件の[62]。

³² *I-Admin* 事件の[73]。

³³ *I-Admin* 事件の[79]。

が原告に与えられることを確保できるという柔軟性を裁判所が持つようになるという意味において、大きな進展である。

6.3 まとめ

- **I-Admin** 事件についての控訴裁判所は、伝統的な **BOC** のテストを修正し、被告が秘密情報の不正な使用を行ったことを原告が立証しなければならない、という原告の義務を無くした。
- **I-Admin** 事件で示された 2 つの要素を原告が立証した場合、立証責任は被告に移り、自己の良心に影響がなかったことの立証を行わなければならない。これは被告による使用の証拠を得ることが一般に原告にとっては難しいという立証の困難性に対応したものである。
- **I-Admin** 事件では、**BOC** に基づく請求において衡平法上の損害賠償が利用可能であることを明らかにした。これにより裁判所は、損害額の算定について、事案に応じて適切な決定を行う広い裁量を持つことになる。

III. 第2部：漏洩防止のための実務的な対策

(1) シンガポールにおける秘密情報管理の手順

営業秘密を管理するための 4 つの重要なステップは、次のとおりである

- 自社において保有・管理する営業秘密の特定（保護すべき情報の選択及びその重要性の分類）
- 営業秘密のカタログ又はリストの作成・維持（現行の管理システムの確認）
- 保護のための契約上、物理的、技術的な、組織上の措置の実施（情報管理のための具体的なシステム）
- 不正が起きた場合の対応計画の立案

以下、シンガポールに特有の問題に対応するために行うべき、営業秘密管理の実例・システムについて解説する。

(A) 営業秘密の特定

営業秘密には、アイデア、プロセス、製品作成、レシピ、方法論、計画、データ、ソフトウェアなど、膨大な情報が含まれる。営業秘密を特定することで、企業は営業秘密を完全に保護することで得られる価値を認識することができる。そのため、企業は、保護する価値のあるすべての営業秘密を特定するべきである。リスト又はインベントリが作成されれば、企業はそこから保護に値すると考えるものを選び、関連費用決定することができる。

まず、営業秘密を特定し、これに見合うレベルの保護を特定するために、以下の点を検討すべきである。

- これらの「秘密」は、関連する法の下で、営業秘密に該当する
のか？
 - この情報は、どの程度（企業の内外において）知られている
のか？
- (i) 秘密情報と従業員の経験・技能との境界を明確にすることは可能か？

- (ii) 競業他社が情報を独自に情報を獲得するために利用しなければならないリソースはどの程度か？
- (iii) 情報を完成させるのに要した努力（時間、人的資源、金銭的なリソース）はどのようなものであったか？
- 営業秘密としての管理は、正しいアプローチか（特許、著作権、意匠等などに比して）？
- 企業がアクセスできるものであって、かつ保護・維持する義務を負っている第三者の営業秘密は存在しているか？

(B) 営業秘密のカタログを作成し、維持する

次に、企業が保有する営業秘密の種類及びアクセス可能な第三者の営業秘密に関連する情報を記載したカタログを作成すべきである。これは以下の点を含める必要がある。

企業が保有する営業秘密の種類

企業がアクセス可能な、第三者の営業秘密

秘密情報が使用・保管される国と地域

営業秘密が自己の所有であるのか、またはライセンスされているか

どの当事者がどの営業秘密にアクセスしているか

各営業秘密を保護するために実施されている措置

有効期限（又は失効する可能性のある期限）

営業秘密の分類（重要性により低、中、高レベルの区別）

各営業秘密について、定期的な見直し日の設定

このリストは、関連する営業秘密の所有権及び権益を確立し、証明するのに役立つもので、企業が保護を必要とする営業秘密につきさらに認識を持つのに役立つものとなる。

(C) 保護のための契約上、物理的、技術的な組織上の措置（情報管理のための具体的なシステム）を実施する。

次に、企業は、組織内での営業秘密の不必要な複製・共有を最小限に

抑えるために、リスク管理マニュアルと手続きを実施すべきである。これらの措置は、営業秘密の不正アクセス、使用、開示、喪失及び改ざんを防止し、従業員のための明確なマニュアル及びガイダンスを提供し、そして第三者の営業秘密に関して課された義務の違反を回避するのに役立つ。

このようなマニュアルやポリシーは、組織内、そしてパートナー企業のネットワーク内での協力と透明性を促進する必要性とのバランスをとる必要があると考えられる。

以下、組織的な保護措置として導入することが推奨される措置を記載する。

- 適切に設計され、実施されたポリシー及びマニュアル、並びに並びに秘密保持義務に関する、従業員に対する定期的な指導・教養等のトレーニング。
- 適切なソフトウェア等を使用した、企業内実務の頻繁なモニタリングにより、プロトコルとポリシーが遵守されていることの確認。
- 当該従業員がその情報を知る必要が本当にあるか、という観点からの秘密情報へのアクセス制限と、かかるアクセス制限の記録の保持。
- 物理的な障壁、鍵の掛かる仕組み、ペーパーシュレッダーの実施。
- パスワード、ファイアウォール、自動侵入検知システム、及び組織の特定の活動に合わせた認証手段を含む技術的な安全対策の実施。
- 労働契約内の規定など、営業秘密の保護を支援するために必要な雇用関係上の規定の実施。
- 退社時の面談で機密保持義務を理解し遵守していることの確認、及び、退社時に機密情報を保持していない旨の誓約書への署名をすること。
- 情報を秘密として保持することに関する、従業員への実践的な指導。たとえば、公共交通機関、エレベーター、トレードショ

一、カンファレンスなどで企業の業務について話し合いをしないよう従業員に助言したり、公共の場所で仕事に関連する機器を使用する際には注意を払うよう助言したりすることが考えられる。

- 従業員が機密情報にアクセスする際に、営業秘密を第三者と共有することに関連して、秘密保持契約や機密保持契約など必要な契約条項を入れこみ、契約の締結に当たってフォローアップすること。
- 契約を定期的に見直し、常に従業員の役職に合ったものとし、適切な保護を提供することを確保すること。
- 企業の秘密情報に関連した、顕著な又は注目すべき開発行為について、並行して書面での記録を維持し、口頭で従業員に開示された情報についても記録を維持すること。
- 適切な場合、競業避止契約を使用すること。秘密保持契約は、主要な研究開発活動の従業員が不適切な使用又は開示を行うことを防止するには不十分である場合がある。それに対して競業避止契約は、営業秘密を使用又は開示する機会を最小限にするために、従業員のその後の活動に一定の線を引くことにより、より広範な保護を提供することができる。
- 秘密であることを示す通知の使用。文書資料に「機密」と表示すること（透かしや冒頭などに）等を検討する。これは、秘密情報を含む技術図面や文書を取り扱う際に特に重要である。
- 異なるレベルの機微性を有する情報に対し、異なる水準の保護措置を取ることを検討すること。
- 営業秘密とノウハウと個人情報保護に関するグループ全体のポリシーを展開すること。
- 現在の手順が適切であるかどうかを判断するために、セキュリティの手続きを頻繁に見直し、内部監査又は外部監査を実施すること。
- 訴訟又は仲裁におけるディスクロージャー、ディスカバリー、又は文書作成の義務について、かかる紛争が生じた場合には、

適宜これを確認すること。

- 営業秘密に関する契約には、紛争解決に関する適切かつ効果的な条項を設けること。企業としては、秘密情報や営業秘密に関連した契約から生じる全ての紛争について仲裁で解決するという条項を設け、手続きを秘密にするのが望ましいであろう³⁴。

また、新型コロナの蔓延により、リモートワーキングが必要となっているが、企業はその IT システムがそのような変更をサポートできるかを確認し、増大するサイバーセキュリティと個人情報についてのリスクに対応することが必要となっている。企業として、これらのリスクに対応するために導入するべき点について、以下、記載する。なお、附属書 E の、リモートワークにおけるチェックリストも参照のこと。

- **制限されたシステムへのアクセス**：つい最近までは、オンプレ環境でのみアクセス可能なシステムのみを有していた企業がほとんどであった。リモートワーキング環境への変化に伴い、多くの企業がリモートアクセスのためにシステムを解放したが、システムのインテグリティを保つためには、当該システムが適切に設定され、リモートアクセスのための追加の認証手続き（例えば、二要素認証）を導入することが必要である。
- **リモートワーキングのための IT リソース**：リモートワーキング実現のために従業員用の追加のデバイスを導入した場合、これらが最新のセキュリティソフトを備え、さらに必要なセキュリティパッチが適用されていることを確実にする必要がある。もし従業員に、リモートワークのために従業員の私的なデバイスを使用することを許可するのであれば、その使用についての明確なルールを作成し、特に、企業が保有する情報のダウンロード及び拡散について規定することが必要となる。
- **リモートでの接続**：リモートでの接続数の増大により、不正な目的での接

³⁴ シンガポール国際仲裁センターのモデル条項・サンプルにおける仲裁合意には、以下の記載がある。「本契約に起因または関連する紛争は、その存在、有効性または終了に関する疑義を含め、その時点で有効なシンガポール国際仲裁センター（「SIAC」）の仲裁規則（「SIAC 規則」）に基づきシンガポール国際仲裁センターが管理する仲裁に付され、仲裁により最終的に解決されるものとする。当該規則は、本条において言及することにより組み込まれるものとみなされる。仲裁地は、[●シンガポール]とする。仲裁裁判所は、[●]人の仲裁人で構成されるものとする。仲裁の言語は、[●]とする」。なお、[●]が付された部分の文言は、両当事者の合意に応じて、適宜括弧内に記入するものとする。この点の詳細については、<https://www.siac.org.sg/model-clauses/siac-model-clause> を参照のこと。

続が目立たなくなる危険性がある。もし従業員が安全ではない、又は汚染された接続手段をリモートワークに使用した場合（例えば、カフェでのインターネット接続など）はなおさらである。企業としては、このようなリスクへの体側、例えば安全な接続経路でのみアクセスを認めるなどの適切な対応を取ることが必要となる。

このような安全管理措置の信頼性維持のため、企業としては営業秘密管理のシステム又は監視のために、特定の部署又は責任者を置くべきである。

(D) 不正な流用などに対応するプランの立案

最後に、企業は、営業秘密の不正な流用に対処するための計画を策定すべきである。これは、避けられないセキュリティ侵害行為に備え、企業が修復不能な被害を被ることを防止し、営業秘密が急速に流布することを防止するために迅速に行動することを可能にするためである。対応の遅れは、前述の暫定的な差止命令及びその他の暫定的救済を得られるかという企業の能力に影響を与える可能性がある。

対応プランは、以下のような内容を備えるべきである。

- 違反の種類に応じた適切な措置を講じるために、違反をランク化し、又は分類する方法を定める。
- 違反が発生した場合、誰に通知すべきかを特定する（社内のアドバイザー（例えば経営層、社内弁護士、広報、HR、IT 部門など）及び社外のアドバイザー（外部弁護士、フォレンジック調査の専門家など）を含む）。
- 営業秘密（又はその中の一定の種類 of 営業秘密）へのアクセスを停止又は制限するための措置を設定する。
- 誰が、どのように違反の詳細を調査し、文書化するか、特定する。
- 違反に対する救済手段を求める措置を設定する。
- どの部署が、どの措置を講じる責任を負うかを特定する（理想的には、IT 担当者、取締役、弁護士、記録の管理責任者、及び必要に応じて広報スタッフが関与する分野横断的なアプローチをとる）。

- 個人情報保護法の下での要件に関する特別な考慮事項を含める。これらの制度は営業秘密や他の知的財産制度とは異なるためである。
- 不正流用に対する行動計画に基づく責任者に簡単にアクセスできるようにする。
- 不正流用に対する行動計画の効果的な実施を確実にするためのトレーニングプログラムを含め、演習訓練を実施する。
- 関連するすべての法律及び業務上の考慮要素に基づき、定期的に更新する。

(2) 秘密情報に関する契約書作成上の留意事項

秘密情報の保護に関する契約・契約条項を作成する際に留意すべきいくつかのポイントを以下に記載する。

2.1 秘密保持条項

秘密保持原則に基づいて保護される商業情報は、多くの形態をとりうる。ほとんどの種類の情報が、商業情報及び個人情報を含む秘密情報の対象となり得る。従って、コモンローの下では、秘密情報の網羅的なリストは存在しない。ある情報が秘密情報であるか、営業秘密であるかは、当該情報の性質及びその他の要素、例えば企業にとっての商業的な価値などによる。

秘密情報の例をいくつか挙げると、以下のとおりである。

- 最終製品においては分析することができない製法
- 最終製品からは明らかとならないレシピ
- プロセス（例えば、発酵技術など）
- ビジネス方法（公共の場で使用されるようになるまで）
- 財務情報
- 統計情報
- 顧客及びサプライヤーのリスト、連絡先情報及びデータ
- 設計、スケッチ及び図面

- 製品・工程の改善
- 特許出願中の新規発明
- 事業計画
- コンピュータプログラム
- 発見、科学的な理論又は数学的な方法

秘密保持契約には、常に以下のような重要な条項が含まれているべきである。これは、秘密保持契約、雇用契約、ライセンス契約、ディストリビューション契約、フランチャイズ契約、及び秘密又は機微な情報が交換される当事者間のその他の商業契約を含む、あらゆる種類の契約に適用される。

- **「秘密情報」の適切な定義**

秘密情報として保護されるようにするためには、当該情報は必要な秘密性を有していなければならない。企業は、その事業の性質及び他者との取引を考慮して、企業が保護しようとする対象の秘密情報を考えなければならない。「秘密情報」の定義は、受領当事者に対する情報の意図的又は不注意による開示並びに秘密情報に由来する成果物をカバーするのに十分に広くなければならない。当然、受領当事者は、この定義を可能な限り狭く維持することを望むと考えられる。また、資料が真に秘密でなくなった場合（すなわち、必要な程度の秘密性を失った場合）、これに反する契約の文言があっても、その事実を変更することはできない。秘密情報の定義において、情報が保護されなくなる特定の状況を記述する明示的な言葉を含めることにより、これを確認することが通常である。（附属書 C の 1 条(f)及び 3 条を参照のこと。）

- **情報を秘密に保持するという中心的な義務と、許可された目的にのみ使用する義務**

秘密保持の中心的な義務に加えて、開示当事者は、受領当事者が情報を使用できる目的を明確に規定すべきである。

- **開示当事者（A）が受領当事者（B）に対して、他の当事者への情報開示を許可する状況及びその相手方**

通常、当事者（B）による従業員及びアドバイザーへの営業秘密の開示は許される。当事者（A）は、秘密情報を受領する当事者（B）のすべての従業員及びアドバイザーに対し、別途、秘密保持契約に署名するよう要求することができる。この方法は、一般的には、煩雑であると思われることもある。一方で当事者（B）がその従業員又はアドバイザーによる秘密保持違反に対して責任を負う方法としては合理的であるといえる。適用される法律や規制の下で必要とされる当事者（B）による開示は、常に許可されるべきである。

- **ディール、プロジェクト、取引が実現しない場合、又は終了に至った場合、情報と記録はどうなるか**

開示当事者は、プロジェクト又は取引が進行しない場合の、又は場合によっては要求に応じての、秘密情報の返却又は破棄について規定すべきである。ただし、受領当事者は、秘密情報を含む一定の記録を維持することを法律上要求されることがある（取締役会議事録など）。

- **契約の存続期間**

秘密情報は、その秘密性を保持する限り、秘密情報として保護することができ、理論的には無期限に保護することができる。しかし実際には、例えば以下のような、多くの制約がある。

- (i) 情報は、時代遅れになり、商業的価値を失うことによって、真の秘密性を失うことがある。動きの激しい業界では、このことは、秘密が比較的短期間しか価値を持たないことを意味するかもしれない。
- (ii) 秘密保持契約又は非開示契約は、通常、期限が限定されている。
- (iii) 元従業員の場合、守秘義務は、元従業員の契約における制限条項と同様の期間は当然に継続すると見なされるであろうが、その義務を退職後にも強制することには困難があるかもしれない。

技術情報は、ほとんど無期限に商業的価値を維持することができるが、ビジネス上の情報は、短期間しか価値を維持できない

場合がある。従って、両当事者は、保護される情報の種類に関連して、契約の期間について現実的な期間を設定すべきである。

2.2 競業避止条項及び勧誘禁止条項

秘密情報、特に営業秘密の保護は、取引制限に関する条項を正当化することができる理由として認められている。営業秘密の保護には、主に2つの方法がある。

- 契約上の秘密保持契約（独立した契約としての秘密保持契約又は非開示契約（NDA）であるか、又は商業的な契約の中に含まれる秘密保持条項又は非開示条項であるかは問われない）
- 制限条項

秘密保持契約（又は NDA）、又は契約条項には、非勧誘条項、開示当事者の従業員又は顧客を勧誘することを一方の当事者に制限する条項、又は競業避止条項（一方の当事者が企業を退職した後に競合他社に参与する、又は利害関係を持つ、勤務する、又は他の方法で取引することを制限する。）などの制限条項が含まれる場合がある。ただし、そのような制限条項が有効となるためには、以下の原則が適用される。

シンガポールでは、当該条項を強制しようとする当事者が以下のことを証明できない限り、制限条項は強制不能であるというのが原則的な立場である。

- 当該条項は、強制しようとする当事者の正当な利益を保護するものであること。使用者が制限条項を通じて保護しようとする正当な利益は、一般に、(i)営業秘密又は営業秘密に類似する秘密情報³⁵、(ii)顧客、顧客又はサプライヤーのような取引関係を保護するという利益³⁶、及び(iii)安定した熟練の労働力を維持す

³⁵ 雇用契約にすでに営業秘密または秘密情報を保護する明示的な秘密保持条項が含まれている場合、たとえ従業員であった者が雇用の過程で営業秘密または機密情報にアクセスしていたとしても、このことは制限条項を正当化するものではない。*Lee Gwee Noi*, [66] を参照のこと。

³⁶ 十分な正当事由として取引関係に依拠するためには、会社は、従業員がその顧客について、事業を指揮する場所において現実に影響を及ぼし、または将来影響を及ぼす可能性のある、個人的知識および影響力を有していたことを証明しなければならない。

るという利益³⁷、の 3 つである

- 制限は、当事者の利益のために合理的であり、かつ、公共の利益のために合理的であること³⁸。

したがって、企業は、雇用契約において、企業における特定の従業員の役割及び影響力、秘密情報及び営業秘密へのアクセスに照らして絞り込まれ、かつ企業の正当な利益を保護するために必要な範囲でのみ従業員を制限するような方法で、制限条項を作成するよう、注意すべきである。

2.3 分離条項

シンガポールの裁判所では、分離の原則は、限られた状況において、また制限条項を有効にするために制限条項の一部を削除しても当該条項に文法上の問題が生じない場合にのみ適用される。シンガポールの裁判所は、両当事者の合意した条項を書き直すようなことはしない。しかし制限条項の中の、違反部分の分離に関するこの条項は、抑止効果のために、依然として契約に残してもよいだろう。

2.4 準拠法及び裁判管轄条項

秘密保持契約に準拠法及び管轄条項が含まれる場合、その秘密保持契約にどの準拠法及び管轄が適用されるかについて、シンガポール法は規定していない。両当事者は、準拠法及び裁判管轄について合意することができる。

準拠法及び裁判合意管轄条項がない場合、当事者は、抵触法の原則に従って、当該契約に適用される準拠法及び合意裁判管轄権を主張しなければならない。

第 1 部(2)に記載の「秘密情報に関する契約書作成上の留意事項」は、シンガポール法が該当の契約に適用されることを前提としていることに留意されたい。

(3) 漏えい事案への対応

詳細については、上記第 1 部の(4)（「救済手段」）及び第 2 部の

³⁷ *Man Financial (S) Pte Ltd v Wong Bark Chuan David* [2008] 1 SLR(R) 663, [94].
³⁸ *Lek Gwee Noi v Humming Flowers & Gifts Pte Ltd* [2014] 3 SLR 27 ("Lek Gwee Noi"), [34].

(1)(1)(D)（「不正な流用などに対応するプランの立案」）を参照のこと。

セキュリティリスク又は事案を特定し、適時に対応するためには、下記の点を含んだ対応計画を策定しておく必要がある。各項目について、企業が対応できているか、チェックする必要がある。

項目	チェックリスト
システム上の動きが常にモニタリングされており、疑わしいリスク、危険又は事案の発生があった場合、各所に通知されるプロセスができている。	
事案の発生が通知された場合、それが真に危険性のある事象であるかを調査し判断する内部のプロセスが導入されている	
調査の内容及び結果が書面化されるプロセスが導入されている	
不正な使用又は漏えい（不正アクセス又は不正なダウンロード）についての証拠を、企業の記録から保存するプロセスが導入されている	
必要な場合、外部専門家（外部の弁護士、コンピュータのフォレンジック調査のチーム）への相談を行うことができる	
内部への必要な連絡（ディスカバリー制度に対応したリティゲーションホールドの通知、経営層への報告など）がなされるようになっている	
当局（個人情報保護又はサイバーセキュリティ関連の当局）への開示が必要であるかを判断するプロセスがある	

各事案により、適切な救済手段(例えば、刑事及び民事手続き、裁判によらない紛争解決手続きなど)を判断できる(詳細については、上記第Ⅰ部(4)を参照。)	

II3.2III(1)0

(4) 参考資料:関連文書等のフォーマット例

以下の文書のためのいくつかのサンプル条項を本書の附属書として添付する。

- 附属書 A : 企業のポリシーにおける秘密保持条項の例
- 附属書 B : 雇用契約における競業避止条項の例
- 附属書 C : 取引先との間の秘密保持契約書における秘密保持条項の例
- 附属書 D : 企業内施設への訪問者に対する秘密保持義務の通知の例
- 附属書 E : リモートワークのためのサイバーセキュリティとデータ保護チェックリスト

これらのサンプル条項は、シンガポール法が該当の契約に適用されることを前提として作成されていることに注意されたい。これらの条項は、例示的な目的のみを目的としており、関連する文脈、従業員、秘密情報の種類及びシナリオに合わせて変更することなく無差別に使用されてはならない。

附属書 A

企業のポリシーにおける秘密保持条項の例

注:これは、企業のポリシーにおける秘密保持条項の例です。必要に応じて変更した上でご使用ください。

1. As part of our workforce, you have a duty to keep our Company's assets confidential, protect them from unauthorised use or loss, and to use them only for legitimate business purposes. Disclosure of our confidential information can cause our Company substantial damage.
2. Some examples of confidential information include:
 - (a) Non-public research, technical data, trade secrets, and other non-public intellectual property;
 - (b) Non-public products, business or marketing plans;
 - (c) Proprietary software code, formulas, drawings, designs, recipes;
 - (d) Non-public financial and forecasted information relating to shipment, revenue, margin, product and costs;
 - (e) Information relating to customer sales, customer contacts and customer behaviour and other confidential customer information;
 - (f) Information relating to supplier metrics, contacts, data and other confidential supplier information; and
 - (g) Employee information such as salaries and organisational charts.
3. Every employee should take appropriate measures to protect the Company's confidential information in the following ways:
 - (a) Store all confidential information in a way that is not seen or accessible by persons who do not need access to that information;
 - (b) When you are away from your desk, lock documents that contain confidential information in a cabinet or drawer. If reviewing soft copies of documents that contain confidential information, lock your electronic devices;
 - (c) Carefully review and comply with our company policies regarding

confidential information;

- (d) Consider your audience whenever communicating anything within the Company or to external parties. In particular, double check messages, attachments and recipients prior to sending them to prevent unintentional dissemination of confidential information; and
 - (e) Hold all confidential and/or proprietary information in strictest confidence at all times during your employment and thereafter.
 - (f) [●If applicable] Before sharing any confidential information with an outside party, in writing or orally, ensure an appropriate Non-Disclosure Agreement (“NDA”), approved by the Company, is in place.
- 4. Third Party Confidential Information. Treat the confidential information of third parties in accordance with the law, contractual agreements with such third parties, and the highest business standards. If you obtain third party confidential information pursuant to an NDA, be sure to comply with the terms of that NDA.
 - 5. Customer Confidential Information. Information that belongs to our customers which is not intended for public distribution is generally considered customer confidential information. This information may or may not have been disclosed under an NDA. In addition, our customers' contracts may specifically preclude us from mentioning that they are our customers. You must follow the confidentiality requirements specified by our customers.
 - 6. Competitor Confidential Information. Be very careful when you are having conversations with people who work for competitors, to avoid receiving any confidential information from them. Obtain any information regarding our competitors legally and ethically.
 - 7. Unauthorised use or disclosure of another party's confidential information or trade secrets may result in civil and criminal consequences. Please approach the [●Human Resources Team] if you have any questions regarding the above.

< 参考和訳 >

1. 当社の従業員の一員として、貴殿は、当社の資産を秘密に保持し、それらを不正使用又は喪失から保護し、それらを正当な事業目的のためにのみ使用する義務を負います。当社の秘密情報を開示することは、当社に重大な損害を与える可能性があります。
2. 秘密情報の例としては、以下のものがあります。
 - (a) 非公開の研究、技術データ、営業秘密、その他の非公開の知的財産
 - (b) 非公開の製品、業務又はマーケティング計画
 - (c) 独自のソフトウェアコード、製法、図面、デザイン、レシピ
 - (d) 出荷、収益、マージン、製品及びコストに関する非公開の財務情報及び予測情報
 - (e) 顧客への販売、顧客との連絡先、顧客の行動、その他の顧客の秘密情報に関連した情報
 - (f) サプライヤーの指標、連絡先、データ及びその他のサプライヤーの秘密情報に関連する情報
 - (g) 給与や組織図などの従業員情報
3. すべての従業員は、当社の秘密情報を保護するための、以下のような適切な措置を講じなければなりません。
 - (a) すべての秘密情報を、当該情報にアクセスする必要のない者が閲覧又はアクセスできない方法で保管すること。
 - (b) デスクから離れる場合は、秘密情報を含む文書をキャビネット又は引き出しに施錠すること。秘密情報を含む文書のソフトコピーをレビューする場合は、電子デバイスをロックすること。
 - (c) 秘密情報に関する当社のポリシーを慎重に検討し、遵守すること。
 - (d) 企業内部、又は外部と何らかのコミュニケーションをする場合は常に、聞く相手を考えること。特に、メッセージや添付文書、及び受領者を送信前にダブルチェックし、意図しない秘密情報の流布を防止すること。

- (e) 全ての秘密情報・専有情報を、在職中及びその後も常に、厳格に秘密として保持すること。
 - (f) **[●該当する場合]**秘密情報を外部当事者と文書又は口頭で共有する前に、当社が承認した適切な秘密保持契約書(「**NDA**」)が締結されていることを確認すること。
- 4. **第三者の秘密情報。**第三者の秘密情報については、法令、第三者との契約のほか、最高レベルの業界標準に従い取り扱うこと。貴殿が秘密保持契約に基づいて第三者の秘密情報を取得する場合、当該秘密保持契約の条件を必ず順守すること。
 - 5. **顧客の秘密情報。**当社の顧客に属する情報であって、公表を目的としないものは、一般に顧客の秘密情報とみなされます。当該情報は、秘密保持契約に基づいて開示される場合も、基づかない場合もあります。さらに、当社の顧客の契約は、当社が顧客であることを言及することを特に禁止している場合があります。貴殿は、当社の顧客が指定する秘密保持の要件に従わなければなりません。
 - 6. **競業他社の秘密情報。**競合他社のために働いている人と会話をするときは、秘密情報を受け取らないように十分注意してください。競合他社に関する情報は、適法に、また倫理に沿って入手してください。
 - 7. 相手方当事者の秘密情報又は営業秘密を不正に使用又は開示すると、民事上及び刑事上の結果を招くことがあります。上記についてご不明な点がある場合は、**[●人事チーム]**まで問い合わせてください。

附属書 B

雇用契約における競業避止条項の例

注:これは、雇用契約における競業避止条項の例です。必要に応じて変更した上でご使用ください。

1. The Singapore High Court case of Tan Kok Yong Steve v Itochu Singapore Pte Ltd [2018] SGHC 85 provides a useful example of an enforceable non-compete clause. There, the Court upheld a non-compete clause that extended to Vietnam and Philippines for a period of 2 years. This was the first decision in over a decade that the Singapore Courts enforced a 2-year non-compete clause. Please note that the Court found that the activity scope, geographical scope and the temporal scope of the restraint of trade clause was reasonable between parties and not against the public interest, given the ex-employee in question's role and activities at the ex-employer and the restraints in question.

2. The non-competition clause in that case stated:

“The Employee hereby agrees and undertakes that during the Employment and for a period of 2 years (Two Years) after termination of the Employment, the Employee will not, without the Employer's prior written consent, directly or indirectly, whether for the Employee's own account or for the account of any other party, be employed or engaged in any capacity or otherwise be interested in or involved with any company or business which competes with the Employer and/or any Affiliate in respect of Restricted Goods or Restricted Services within the Restricted Area.

...

“Restricted Area”

means the area (geographical or otherwise) constituting the market of the Employer and that of any Affiliate for the Restricted Goods and Restricted Services;

“Restricted Goods”

means any product competitive with any product sold or supplied by the Employer and/or any Affiliate with which the Employee

was concerned during the period of 12 months immediately preceding the date of termination of the Employment;

“Restricted Services”

means any services competitive with any of the services sold or supplied by the Employer and/or any Affiliate with which the Employee was concerned during the period of 12 months immediately preceding the date of termination of the Employment.”

<参考和訳>

1. シンガポール高等裁判所の事件 *Tan Kok Yong Steve v Itochu Singapore Pte Ltd* [2018] SGHC 85 は、強制可能な競業禁止条項の有用な例を提供している。この事件で裁判所は、ベトナムとフィリピンにまたがり、2 年間という期間の競業禁止条項につき、これを有効とした。これは、シンガポールの裁判所が、最近 10 年以上の期間で初めて、2 年間の競業禁止条項を強制力があるとした判決である。裁判所は、当該元従業員の役割、前雇用者での活動、及び該当の制限を考慮すると、取引制限条項における活動の範囲、地理的範囲及び時間的範囲は、当事者間において合理的であり、公益に反するものではないと判断した。
2. その事案における競業禁止条項は、以下のように規定していた。

「従業員は、ここに、本雇用期間中及び本雇用の終了後 2 年間、雇用主の事前の書面による同意なしに、直接にも間接にも、従業員自身の計算によるか他者の計算によるかを問わず、制限地域内において、制限商品又は制限サービスに関して雇用主又は関連会社と競合する企業又は事業に雇用され、いかなる立場としても契約し、又はその他利害関係を有したり、関与しないことに同意し、約束する。

...

「制限区域」

とは、雇用者及び関連会社の制限商品及び制限サービスの市場を構成するエリア(地理的又はその他)を意味する。

「制限商品」

とは、雇用の終了日の直前 12 ヶ月間に従業員が関係していた雇用主及び又は関係会社が販売又は供給した製品と競合する製品を意味する。

「制限サービス」

とは、雇用の終了日の直前 12 ヶ月間に従業員が関係していた雇用主及び又は関連会社が販売又は供給したサービスと競合するサービスを意味する。

附属書 C

ビジネスパートナーとの秘密保持契約における秘密保持条項の例

注: これは、秘密情報を開示する当事者(「開示当事者」)とそれを受領する当事者(「受領者」)との間で締結される NDA の秘密保持条項のサンプルです。必要に応じて変更した上でご使用ください。

1. “Confidential Information” means all confidential information relating to the [state the purpose for which the agreement is entered into, e.g. the evaluation or establishment of a collaboration in respect of a particular project] (the “Purpose”) which the Disclosing Party directly or indirectly discloses to the Recipient [before, on or after the date of this agreement]. This includes:
 - (a) The fact that discussions and negotiations are taking place concerning the Purpose and the status of those discussions and negotiations;
 - (b) The existence and terms of this agreement;
 - (c) All confidential or proprietary information relating to:
 - (i) The business, affairs, customers, clients, suppliers, plans, intentions, or market opportunities of the Disclosing Party; and
 - (ii) The operations, processes, product information, know-how, technical information, designs, trade secrets or software of the Disclosing Party;
 - (d) Any information, findings, data or analysis derived from Confidential Information; [and]
 - (e) Any other information that is identified as being of a confidential or proprietary nature;
 - (f) But excludes any information that:
 - (i) Is, or becomes, generally available to the public other than as a direct or indirect result of the information being disclosed by the Recipient in breach of this agreement [(except that any compilation of otherwise public

information in a form not publicly known shall still be treated as Confidential Information)];

- (ii) Was available to the Recipient on a non-confidential basis prior to disclosure by the Disclosing Party;
 - (iii) Was, is, or becomes available to the Recipient on a non-confidential basis from a person who, to the Recipient's knowledge, is not under any confidentiality obligation in respect of that information;
 - (iv) Was lawfully in the possession of the Recipient before the information was disclosed by the Disclosing Party;
 - (v) Is developed by or for the Recipient independently of the information disclosed by the Disclosing Party;
 - (vi) The parties agree in writing that the information is not confidential.
2. Confidentiality Obligations. The Recipient will keep secret and retain in strictest confidence, and will not, without the prior written consent of the Disclosing Party, furnish, make available, or disclose the Confidential Information to any third party. Unless otherwise provided in this agreement, the Recipient shall not make use of the Confidential Information for its own commercial uses or for the benefit of any third party, and shall use the Confidential Information only for the purposes for which this agreement is entered into.
3. Confidentiality Period. This agreement and the Recipient's duty to hold Confidential Information in confidence shall survive until [●date].
4. Standard of Care. The Recipient shall protect the Confidential Information received hereunder from disclosure to any unauthorised person, firm, corporation or other third party by using the same degree of care that it uses to prevent the unauthorised disclosure of its own confidential information of a like nature, but in no event less than a reasonable degree of care.
5. Return or Destruction of Confidential Information. If so requested by the Disclosing Party at any time by notice in writing to the Recipient, the Recipient shall:

- (g) Destroy [or return to the Disclosing Party] all documents and materials [(and any copies)] containing, reflecting, incorporating or based on the Disclosing Party's Confidential Information;
- (h) Erase all the Disclosing Party's Confidential Information from its computer and communications systems and devices used by it, or which is stored in electronic form; [and]
- (i) [To the extent technically and legally practicable,] erase all the Disclosing Party's Confidential Information which is stored in electronic form on systems and data storage services provided by third parties; and
- (j) Certify in writing to the Disclosing Party that it has complied with the requirements of this Clause.

Nothing in this Clause shall require the Recipient to return or destroy any documents and materials containing or based on the Disclosing Party's Confidential Information that the Recipient is required to retain by applicable law, or to satisfy the requirements of a regulatory authority or body of competent jurisdiction or the rules of any listing authority or stock exchange, to which it is subject. The provisions of this agreement shall continue to apply to any documents and materials retained by the Recipient pursuant to this Clause.

- 6. Equitable Remedies. The Recipient acknowledges and agrees that in the event of any actual or threatened breach by the Recipient of this agreement, the Disclosing Party will be entitled to seek immediate injunctive and other equitable relief, without bond and without the necessity of showing actual monetary damages. Nothing herein will be construed as prohibiting the Disclosing Party from pursuing any other remedies available to it, including the recovery of any damages that it is able to prove.

< 参考和訳 >

- 1. 「**秘密情報**」とは、[本契約締結の目的、例えば、特定のプロジェクトに関する共同研究の評価又は設立、などを記載]（「**本目的**」）に関連するすべての秘密情報を意味し、開示当事者は、[本契約締結日の前、又は締結日以後]に直接又は間接にこれを受領者に開示する。これには、以下を含む。

- 本目的について協議及び交渉が行われている事実、及びその協議及び交渉の状況
- この契約の存在、及びその条項
- 以下に関連するすべての秘密又は専有情報
 - (i) 開示当事者の事業、業務、顧客、クライアント、サプライヤー、計画、意図又は市場機会
 - (ii) 開示当事者の業務、プロセス、製品情報、ノウハウ、技術情報、デザイン、営業秘密又はソフトウェア
- 秘密情報に由来する情報、知見、データ又は分析
- その他、機密性又は専有性を有すると特定される情報
- ただし、以下の情報は含まない。
 - (i) 本契約に違反して受領者により情報開示されたことの直接又は間接の結果としてではなくして、一般に公知であり、又は公知となった情報。[（公知ではない形式のその他の公開情報の編集物は、依然として秘密情報として取り扱われる。）]
 - (ii) 開示当事者による開示前に受領者が秘密とならない方法で入手可能であったもの。
 - (iii) 受領者が知る限り、当該情報に関して秘密保持義務を負わない者から秘密とならない方法で受領者が入手した、又は入手可能となった情報。
 - (iv) 開示当事者が情報を開示する前に、合法的に受領者が保有していたもの。
 - (v) 開示当事者により開示された情報とは独立して、受領者により、又は受領者のために開発されたもの。
 - (vi) 両当事者が、当該情報が秘密ではないと書面で同意したもの。

2. **秘密保持義務。** 受領者は、秘密性を保持し、厳重に秘密として保管するものとし、開示者の事前の書面による同意なしに、秘密情報を第三

者に提供、提供又は開示しないものとする。本契約に別段の定めがない限り、受領者は、秘密情報を自己の商業的使用又は第三者の利益のために使用しないものとし、秘密情報を本契約が締結された目的にのみ使用するものとする。

3. **秘密保持期間。**本契約及び受領者による秘密情報を秘密に保持する義務は、[●日付]まで存続するものとする。
4. **保護措置の基準。**受領者は、本契約に基づき受領した秘密情報を、同様の性質の自己の秘密情報の無断開示を防止するために使用するのと同程度の注意をもって、ただしいかなる場合にも合理的な程度を下回らない注意をもって、権限のない人物、事務所、法人又はその他の第三者への開示から保護する。
5. **秘密情報の返却又は破棄。**開示当事者が受領者に書面で通知要求する場合はいつでも、受領者は、下記事項を行うものとする：
 - 開示当事者の秘密情報を含み、反映し、組み込まれ、又はそれに基づいているすべての文書及び資料[（及びコピー）]を破棄する[又は開示者に返却する]。
 - 開示当事者のすべての秘密情報を、開示当事者が使用するコンピュータ及び通信システム及び機器、又は電子形式で保管される機器から消去すること。
 - [技術的及び法的に実行可能な範囲において、]第三者が提供するシステム及びデータ保管サービスに電子形式で保存されているすべての開示当事者の秘密情報を消去すること。
 - 本項の要件を遵守したことを書面で開示当事者に証明すること。

本項のいかなる規定も、受領者が適用法により、又は管轄権を有する規制当局もしくは組織の要件、又は対象となる上場機関もしくは証券取引所の規則の要件を満たすために保持することを要求される、開示当事者の秘密情報を含む又はそれに基づく文書及び資料の返却又は破棄を受領者に要求するものではない。本契約の規定は、本項に基づき受領者が保管する文書及び資料に引き続き適用されるものとする。

6. **衡平法上の救済。**受領者は、本契約の受領者による実際の違反又は違反のおそれがある場合、開示当事者が、保証金なしにまた実際の金銭

的損害賠償を示す必要なしに、即時の差止命令及びその他の衡平法上の救済を求める権利を有することを確認し、これに同意する。本契約のいかなる規定も、開示当事者が、開示当事者が証明することのできる損害賠償の支払いを含め、開示当事者が利用可能なその他の救済手段を求めることを禁じるものと解釈されないものとする。

附属書 D

企業内施設への訪問者に対する秘密保持義務の通知の例

注:これは、「訪問者受付」における秘密保持義務の通知であって、公共の場所 / 公共の待合場所/公共の会議室の入口に目立つように表示されるものの例です。必要に応じて変更した上でご使用ください。

[●Company name] (the “**Company**”)

All visitors to the Company’s premises understand that they may be given access to confidential information belonging to the Company through their relationship with the Company or as a result of their access to the Company’s premises.

All visitors understand and acknowledge that the Company’s confidential information and trade secrets consist of information and materials that are proprietary, valuable and not available in the public domain.

All visitors agree to hold in strictest confidence and confidential information and/or trade secrets that they may obtain access to or receive in the course of or by virtue of their access to the Company’s premises. The removal of any document (including soft copies), equipment, or other materials from the Company’s premises without the Company’s authorisation, and/or unauthorised access to the Company’s proprietary information and materials, may result in civil and criminal penalties.

<参考和訳>

[●会社名](「当社」)

当社の施設へのすべての訪問者は、当社との関係に基づき、又は当社の施設へのアクセスの結果として、当社に帰属する秘密情報へのアクセスを許可されることがあることを理解するものとします。

すべての訪問者は、当社の秘密情報及び営業秘密が、専有性があり、価値があり、公知では入手できない情報及び資料で構成されていることを理解し、認識するものとします。

すべての訪問者は、当社の施設へのアクセスの過程で、又はそのせいでアクセスし、又は取得することがある秘密情報及び/又は営業秘密を、最も厳格に

秘密として保持することに同意するものとします。当社の許可なしに、文書（ソフトコピーを含む）、機器又はその他の資料を当社の施設から持ち出すこと、及び/又は企業の専有情報及び資料への権限のないアクセスは、民事的な罰則及び刑事的な罰則を科されることがあります。

附属書 E

リモートワークのためのサイバーセキュリティとデータ保護チェックリスト

注: 上記の第2部(1)(1)(C)の実務ガイドラインに加えて、新型コロナウイルスのパンデミックによるリモートワークの普及に伴い、企業が検討すべきリモートワークのためのサイバーセキュリティ及びデータ保護チェックリストを以下に示します III(1)(1)(C)³⁹。

Cybersecurity and Data Protection Checklist for Teleworking

Item	Completed?
Do we have two-factor authentication in place for remote access?	
Are restricted systems capable of being accessed remotely and appropriately configured?	
Are restricted systems subject to additional layer of authentication or security for remote access?	
Are all remote workers utilizing organization-owned devices for remote access?	
Are those devices fully updated with security software and patches?	
Are remote workers utilising personally-owned devices for remote access?	
Are those devices subject to appropriate security controls?	
Have we prepared our network and workforce for how to address the increased risk in cyber attacks in the remote working context?	
Have we issued appropriate privacy notices and/or obtained suitable consents for our planned monitoring activities?	
Do we need to address privacy terms with any vendors or other third parties that may access the data from our devices?	
Do we need to address any cross-border transfer restrictions that may apply to our workforce's remote access to systems?	

³⁹

詳しくは

<https://www.bakermckenzie.com/en/insight/publications/2020/03/covid19-cybersecurity-privacy-risks-teleworking> をご覧ください。

Do we need to carry out a data protection impact assessment on the proposed data collection and processing activities?	

<参考和訳>

リモートワークのための、サイバーセキュリティ及びデータ保護チェックリスト

項目	完了の有無
リモートアクセスのための二要素認証が導入されているか？	
リモートアクセスが可能となっている制限つきシステムに、適切な設定がなされているか？	
制限つきシステムには、リモートアクセスのための追加的な認証又はセキュリティが導入されているか？	
リモートアクセスをする従業員は、リモートアクセスのために会社所有のデバイスを利用しているか？	
それらのデバイスは、セキュリティソフト及びパッチが完全にアップデートされているか？	
リモートアクセスをする従業員は、リモートアクセスのために個人所有のデバイスを利用しているか？	
それらのデバイスに対して、適切にセキュリティの管理がなされているか？	
リモートワーキングに伴うサイバー攻撃のリスクの増大にどのようにネットワーク及び従業員が対応するか、準備できているか？	
従業員のモニタリングについて、適切なプライバシー通知を出し、十分な同意を得ているか？	
会社のデバイスからデータにアクセスする可能性のあるベンダー及びその他の第三者との間でプライバシーに関する条件について対処する必要はあるか？	
従業員のシステムへのリモートアクセスに当たって適用のある、データの域外移転の制限に対応する必要があるか？	
予定されているデータの収集及び処理の手続きに当たって、データ保護のための影響評価を行う必要はあるか？	

経済産業省委託事業

シンガポールにおける営業秘密管理マニュアル作成

2022 年 3 月

禁無断転載

[調査受託]

Baker & McKenzie. Wong & Leow

独立行政法人 日本貿易振興機構

シンガポール事務所

(知的財産部)

本冊子は、2021年度に日本貿易振興機構シンガポール事務所知的財産部が調査委託を行ったBaker & McKenzie. Wong & Leowが作成した調査報告等に基づくものであり、その後の法改正等によって記載内容の情報は変わる場合があります。また、記載された内容には正確を期しているものの、完全に正確なものであると保証するものではありません。

Copyright(C) 2021 METI/JETRO. All right reserved.

経済産業省委託事業

韓国における営業秘密管理 マニュアル

2022年2月

独立行政法人 日本貿易振興機構
ソウル事務所

目 次

はじめに	1
第 1 編 法制度編	2
第 1 章 営業秘密保護法における営業秘密の定義	2
1. 営業秘密の保護に関連する法制度の概観	2
2. 営業秘密保護法の概要及び沿革	2
3. 営業秘密の成立要件	5
第 2 章 営業秘密保護法における営業秘密侵害行為の定義	7
1. 営業秘密の侵害行為の定義	7
2. 不正取得行為	8
3. 不正取得者からの悪意取得行為	9
4. 事後的関与行為	10
5. 不正公開行為	11
6. 不正公開行為者からの悪意取得行為	12
7. 不正公開行為に関する事後的関与行為	13
8. 営業秘密保護法第2条第1号又目の不正競争行為	14
第 3 章 営業秘密保護法における営業秘密侵害行為類型の事例	15
1. 営業秘密の侵害類型別統計	15
2. 不正取得行為	18
3. 不正取得行為及び不正取得者からの悪意取得行為	19
4. 不正公開行為	21
5. 不正公開行為及び不正公開行為者からの悪意取得行為	23
6. 日韓間の営業秘密侵害紛争の事例	24
7. 新たな侵害形態	26
第 4 章 営業秘密保護のためのその他の制度	27
1. 技術資料任置制度	27
2. 下請取引の公正化に関する法律	27
3. 営業秘密原本証明制度	27
4. 産業技術の流出防止及び保護に関する法律	28
5. 防衛産業技術保護法	28
6. 中小企業保護法	29
7. 刑法	29
8. 商法	30
9. 知的財産基本法	30
第 5 章 営業秘密侵害に対する法的措置及び最近の判例の動向	31

1.	営業秘密侵害に対する法的措置.....	31
2.	最近の判例の動向.....	39
第 2 編	営業秘密漏洩対策実践編.....	43
第 1 章	総論(営業秘密の管理方法).....	44
1.	自主的な営業秘密管理体制の構築.....	44
2.	営業秘密保護センターの営業秘密管理システムの導入.....	47
3.	営業秘密の登録.....	49
第 2 章	管理体制整備のステップ1ー管理体制の現状の確認.....	58
1.	現状把握の必要性.....	58
2.	セルフチェックシート.....	59
第 3 章	管理体制整備のステップ2ー営業秘密情報の洗い出し及び重要度の区分.....	61
1.	営業秘密情報の洗い出し.....	61
2.	重要度の区分.....	62
第 4 章	管理体制整備のステップ3ー管理体制の整備.....	63
1.	担当部門・担当者の設置.....	63
2.	人的(従業員、退職者など)管理.....	63
3.	物的(執務室、生産現場、パソコンなど)管理.....	66
4.	取引先(部外者、ライセンサーなど)の管理.....	70
5.	テレワークの実施に伴う管理上の留意点.....	72
6.	営業秘密の原本証明サービス、技術任置サービスによる管理.....	73
第 5 章	漏洩時の対応.....	75
1.	漏えいの兆候.....	75
2.	初動対応(紛争解決の手順とロードマップ).....	76
3.	民事的解決方法.....	80
4.	刑事的解決方法.....	91
5.	その他の紛争解決方法.....	96
第 3 編	各種関連書類参考書式(フォーム).....	101
1.	内部関係用標準書式.....	102
2.	外部関係用標準書式(1) 外部者との秘密保持契約書の例.....	116
3.	営業秘密保護規定.....	125
4.	主要契約書の韓国語版.....	141

はじめに

本マニュアルは、韓国に進出した日系企業が自社の技術やノウハウを保護するための施策を行う際に役立つよう、営業秘密保護のための韓国の法制度、行政サービス及び実務上の対応方法を紹介するためのものである。

本マニュアルは、日本貿易振興機構の依頼を受けて2015年3月に作成された「営業秘密流出対応マニュアル(韓国)」の改訂版であり、既存マニュアルにおいて、2021年6月23日改正営業秘密保護法を中心に、主な改正事項、営業秘密侵害事例、統計及び判例を変更・追加し、実務上の対応方法に関する内容を追加、補強したものである。

本マニュアルは、大きく3編から構成されている。まず、第1編では、営業秘密保護法を中心に営業秘密保護に関する韓国の法制度を紹介している。第1編では、韓国の営業秘密保護法と日本の不正競争防止法との違いを説明し、韓国の営業秘密保護法に規定された営業秘密侵害行為の類型及び特徴と具体的な事例について紹介する。また、営業秘密侵害行為から営業秘密保有者を保護できる韓国の法律体系及び関連の判例の最新動向について紹介する。また、第2編では、営業秘密流出を防ぐための人的・物的管理体系の構築方法と民事・刑事上の措置を含む流出時の対応方法について詳しく紹介する。さらに、営業秘密漏洩の兆候を把握し、初動対応を通じて営業秘密侵害を最小限に抑えることができる方策等についても紹介する。第3編では、第2編に沿った営業秘密保護体系の構築の際に必要な、秘密保持契約書、営業秘密管理規程など様々な書式の書類作成の際に使用できる標準書式を提供している。

営業秘密として保護される知識資産は、当該企業が長い時間と費用をかけて形成されるものであり、企業収益創出の源泉であるとともに、流出時にはその回収や回復が困難であって、企業に回復できない被害を発生させることになる。したがって、営業秘密が流出しないよう事前に防止することが最善の措置であり、営業秘密が流出した場合、被害がさらに大きくならないよう速やかに対応することが重要である。

しかし、営業秘密保護は国ごとに関連法令や法制度が異なっており、営業秘密保護法に関する知識はもちろん、契約法、証拠法など関連法令に対する理解とともに、民事・刑事訴訟手続についての専門知識が必要となるため、外国に進出する日本企業にとっては戦略的な観点からのガイドラインが必要となる。

一方、韓国の営業秘密保護のための法体系及びこれに関する法解釈は、他国と比べて日本とかなり類似していることが知られており、最近の韓国の営業秘密保護法改正も日本と似た方向性を持って行われている。ただし、韓国で発生している具体的な営業秘密侵害の類型や特徴は、韓国社会が持っている特徴と密接な関係があり、韓国に進出する日本企業は営業秘密の十分な保護のため、このような点を理解することが重要である。

そして、韓国の場合、最近、懲罰的損害賠償制度を導入し、資本金及び経験が不足する中小企業の営業秘密保護体系構築のための行政的支援を強化するなど、大企業から中小企業を保護するための動きを見せている。韓国企業と取引する日本企業にとっては、このような韓国の政策基調を十分に理解し、活用することが望ましい。

本マニュアルは、このような側面を踏まえ、韓国市場への進出や韓国企業との技術交流を考えている日本企業に対し、実務的に有用な情報を提供することに重点を置いて作成された。

本マニュアルが韓国で事業を営む日系企業の営業秘密保護のために少しでも役に立つことを願う。

第 1 編 法制度編

韓国では、営業秘密とは、「公然と知られておらず、独立した経済的価値を有するものであって、秘密として管理された生産方法、販売方法、その他営業活動に有用な技術上又は経営上の情報」をいう。また、健全な取引秩序を維持するために営業秘密を事実上の財産と見なし、「不正競争防止及び営業秘密保護に関する法律」により、他人の営業秘密を侵害する行為を禁止している。

以下本編では、韓国の営業秘密保護制度と不正競争防止及び営業秘密保護に関する法律上の営業秘密の成立要件について詳細に述べる。

第 1 章 営業秘密保護法における営業秘密の定義

1. 営業秘密の保護に関連する法制度の概観

営業秘密は、その営業秘密を保有している企業の経済的価値を決定する重要な要素として認識されている。営業秘密は従来、未公開情報(undisclosed information)、企業秘密又はノウハウ(know-how)など様々な名称で呼ばれているが、これは一般に公開され、一定期間保護される特許発明やその他の知的財産とは対称的な概念であるため、営業秘密を知的財産の一つとして認め、これを保護するか否かについて様々な意見があった。

韓国においては、日本と同様に不正競争防止法の改正により、不正競争防止法において、保護対象となる営業秘密の定義及び営業秘密侵害行為の類型を規定することで、企業と個人の営業又はその活動から発生する営業秘密を保護している。

このように、韓国では営業秘密を保護するための基本法として「不正競争防止及び営業秘密保護に関する法律」を制定しているが、一般法である刑法においても法令による職務上の秘密を保護する規定を設けており、また、民法においても営業秘密を保有する者に対して秘密保持義務を負う当事者が当該義務に違反した場合に、損害賠償責任を課すことで営業秘密を保護する規定を設けている。

また、民法や刑法のような一般法以外にも、「中小企業保護法」や「産業技術保護法」などの特別法により、独自技術保護能力が低い中小企業が保有している営業秘密や、国を挙げて保護が必要な重要技術分野の営業秘密を保護している。

2. 営業秘密保護法の概要及び沿革

韓国は、企業と個人の営業又はその活動から発生する営業秘密を保護するために1991年12月31日、従来の不正競争防止法を改正して「不正競争防止及び営業秘密保護に関する法律」(以下「営業秘密保護法」という。)を制定した。

営業秘密保護法では、①第2条第2号で保護対象である営業秘密の概念を定義する一方、②第2条第3号で営業秘密侵害行為の類型を具体的に定義し、③第10条ないし第12条では営業秘密侵害の発生時に民事的救済手段として、侵害行為の禁止予防請求権、損害賠償請求権及び信用回復措置請求権を規定している。また、④善意の第三者を救済するための特例規定を第13条に設けている。

また、営業秘密保護法は、1991年12月31日の改正以来、2021年6月23日の改正に至るまで累次改正されてきたが、その改正内容を見てみると、改正の趣旨は以下のような方向性を有している。

- ① 営業秘密成立要件の緩和(保護対象の拡大)
- ② 侵害者に対する処罰の強化
- ③ 侵害行為及び侵害主体の拡大
- ④ 懲罰的損害賠償制度の新設

これをより具体的に見てみると、以下のとおりである。

2.1 営業秘密成立要件の緩和(営業秘密保護法第2条第2号)

[表1]

1991. 12. 31. 改正	2018. 4. 17. 改正	2019. 1. 8. 改正
<u>公然と知られておらず、独立した経済的価値を有するものであって、相当な努力により秘密として保持された生産方法・販売方法その他営業活動に有用な技術上又は経営上の情報</u>	<u>公然と知られておらず、独立した経済的価値を有するものであって、合理的努力によって秘密として保持された生産方法、販売方法、その他営業活動に有用な技術上又は経営上の情報</u>	<u>公然と知られておらず、独立した経済的価値を有するものであって、秘密として管理された生産方法、販売方法、その他営業活動に有用な技術上又は経営上の情報</u>
改正の趣旨	中小企業の営業秘密保護を強化し、営業秘密保有者の立証困難を緩和	

2.2 侵害者に対する処罰の強化(営業秘密保護法第18条)

[表2]

	2004. 1. 20. 改正	2007. 12. 21. 改正	2018. 4. 17. 改正	2019. 1. 8. 改正
国内流出 行為	<u>5年以下の懲役又は5千万ウォン以下の罰金</u>	<u>5年以下の懲役又は財産上の利得額の2倍以上10倍以下</u>	<u>5年以下の懲役又は5千万ウォン以下の罰金</u>	<u>10年以下の懲役又は5億ウォン以下の罰金¹</u>
国外流出 行為	<u>5年以下の懲役又は1億ウォン以下の罰金</u>	<u>7年以下の懲役又は財産上の利得額の2倍以上10倍以下</u>	<u>10年以下の懲役又は1億ウォン以下の罰金</u>	<u>15年以下の懲役又は15億ウォン以下の罰金²</u>
国内流出 予備陰謀 行為	<u>2年以下の懲役又は1千万ウォン以下の罰金</u>	-	-	<u>2年以下の懲役又は2千万ウォン以下の罰金</u>
国外流出 予備陰謀 行為	<u>3年以下の懲役又は2千万ウォン以下の罰金</u>	-	-	<u>3年以下の懲役又は3千万ウォン以下の罰金</u>

2.3 侵害行為及び侵害主体の拡大

[表3]

¹ 違反行為による財産上の利得額の10倍に相当する金額が5億ウォンを超えると、その財産上の利得額の2倍以上10倍以下の罰金に処する。

² 違反行為による財産上の利得額の10倍に相当する金額が15億ウォンを超えると、その財産上の利得額の2倍以上10倍以下の罰金に処する。

2004. 1. 20. 改正	2009. 12. 30. 改正	2013. 7. 30. 改正	2019. 1. 8. 改正
処罰対象を従来の該当企業の前・現職の役職員からすべての違反者に拡大。未遂犯と予備陰謀者を処罰。	外国で使用されることを知りながら企業の営業秘密を取得使用した者に対しても第三者に漏えいした者と同様に処罰。	従来、企業が保有する営業秘密を漏えいした者のみ処罰していた規定において、個人や非営利機関を含めた「営業秘密保有者」の営業秘密を漏えいした者を処罰する。	「営業秘密を指定された場所から無断で漏えい」する行為、「営業秘密保有者から営業秘密の削除又は返還を求められても、引き続き保有」する行為も処罰の対象に含む。

2.4 懲罰的損害賠償制度の新設(営業秘密保護法第14条の2第6項)

2019年1月8日の改正では、第14条の2第6項を新設し、営業秘密侵害行為が故意と認められた場合、損害として認められた金額の3倍を超えない範囲で賠償額を決定できるようにし、懲罰的損害賠償制度を新設して、営業秘密の侵害による被害救済を強化した。

韓国の営業秘密保護法と日本の不正競争防止法の主な内容を比較すると、以下の表のとおりである。

[表4]

	韓 国	日 本
営業秘密の保護を担う法令	不正競争防止及び営業秘密保護に関する法律	不正競争防止法
営業秘密侵害罪、罰金刑の上限	国内流出： － 5億ウォン/財産上の利得額の10倍に相当する金額が5億ウォンを超過すると、その財産上の利得額の2倍以上10倍以下 国外流出： － 15億ウォン/財産上の利得額の10倍に相当する金額が15億ウォンを超過すると、その財産上の利得額の2倍以上10倍以下	国内流出： － 個人2000万円 － 法人5億円 国外流出： － 個人3000万円 － 法人10億円
公訴時効(刑事)	10年	7年
営業秘密転得者に対する処罰	営業秘密侵害行為をした者は誰でも処罰対象とする。	不正に公開された営業秘密であることを知りながらその営業秘密を取得した転得者の不正な公開・使用に対しても処罰対象とし、また転得者の処罰を両罰規定の対象ともする。
営業秘密侵害品の流通規制	×	技術上の秘密を使用する行為によって発生した物(営業秘密侵害品)の流通規制
親告罪の有無	× (2004年改正)	× (2015年改正)

		(但し、秘密保持命令違反罪のみ 親告罪)
未遂犯処罰の有無	○ (2004年改正)	○ (2015年改正)
没収規定	×	○ (2015年改正)
推定規定	×	合理的な経験則の範囲及び原告と 被告が立証する負担の公平性等の 観点から一定の条件(営業秘密の 範囲、被告の主観、推定が及ぶ対 象行為)の下に限定して認定
除斥期間・ 消滅時効(民事)	除斥期間 10年 消滅時効 3年	除斥期間 20年 消滅時効 3年

3. 営業秘密の成立要件

韓国の営業秘密保護法第2条第2号では、営業秘密を「公然と知られておらず、独立した経済的価値を有するものであって、秘密として管理された生産方法、販売方法、その他営業活動に有用な技術上又は経営上の情報」として定義している。

したがって韓国においても、WTO・TRIPs協定、EUの営業秘密保護指令や日本の不正競争防止法と同様に、①秘密管理性、②有用性及び③非公知性をその構成要件としている。

特に2019年1月8日改正においては、秘密管理性について、改正前の「合理的努力により秘密として保持された」の要件を「秘密として管理された」に改正し、その要件を緩和することにより、日本における秘密管理性の要件との違いはなくなった。

[表5]

	韓 国	日 本
法 的 根 拠	不正競争防止及び営業秘密に関する 法律第2条第2号	不正競争防止法第2条第6項
非 公 知 性	公然と知られていない	公然と知られていない
有 用 性	独立した経済的価値を持つ	事業活動に有用
秘 密 管 理 性	秘密として管理される	秘密として管理される
保 護 対 象	生産方法、販売方法、その他営業活 動に有用な技術上又は経営上の情報	技術上又は事業上の情報

一方、経済的有用性については、韓国の営業秘密保護法では、日本で規定されていない「独立した経済的価値」を求めていることから、有用性とは別に独立した経済的価値の有無と区分すべきとの見解³がある。しかし、大法院(韓国における最高裁判所に相当)の判決等では、実際の営業活動に利用できるほど完成した状態に至っていない場合でも、営業秘密として認めており⁴、実際に有用性と独立した経済的価値性を区分していない。したがって、日本の不正競争防止法における営業秘密の構成要件と実際的に差がないと見るのが妥

³ キム・グクヒョン、営業秘密保護法実務、世昌出版社 2010、p13-19

⁴ 大法院2008. 2. 15. 宣告2005ド6223判決

当である。

また、保護対象としての技術上の情報は、工業技術に使用されるすべての技術をいうものであって、その情報が有形なのか(模型、図面など)、無形なのか(防水方法、混合方法、処理方法、取扱い方法、ノウハウなど)は問わない。具体的には、技術上の情報としては、設計方法、設計図面、製造方法、製造技術、製造工程、青写真、成分原料と配合比率、強度計算の運用方法、機械の仕様、工場の配置図など、技術に関する情報が挙げられる。

経営上の情報としては、顧客名簿、顧客の管理方法、代理店名簿、材料や商品の購入先、取引先ルート、販売価格表、原価計算表、販売計画、販売指針書、販売マージン率、販売マニュアル、市場調査情報、輸入又は輸出ルート、財産目録、顧客管理技法、経営管理技法、広告や広報計画、宣伝広告方法、未発表の貸借対照表、製品の割引システム、人事や組織及び財務管理技法、非公開の事業計画などが挙げられる。

第 2 章 営業秘密保護法における営業秘密侵害行為の定義

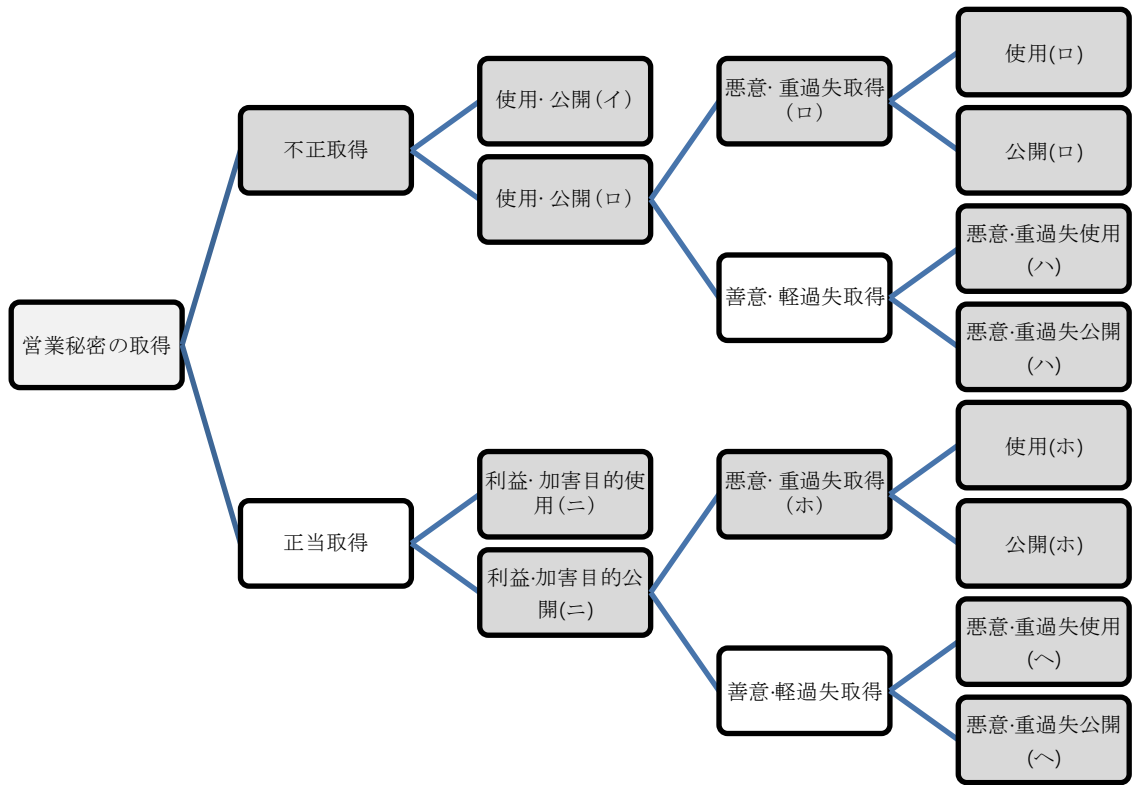
1. 営業秘密の侵害行為の定義

韓国の営業秘密保護法では、営業秘密の侵害行為について、ドイツなどのように一般条項によらず、米国や日本と同様、第2条第3号において営業秘密侵害行為を6つの類型に分けて限定的に示している。

- イ. 窃取、欺瞞、脅迫、その他の不正な手段で営業秘密を取得する行為(以下「不正取得行為」という。)又は、その取得した営業秘密を使用又は公開(秘密を保持して特定人に教えることを含む。以下同じ)する行為
- ロ. 営業秘密に対し、不正取得行為が介入した事実を知ったり、重大な過失により知らないでその営業秘密を取得する行為又はその取得した営業秘密を使用又は公開する行為
- ハ. 営業秘密を取得した後にその営業秘密に対し不正取得行為が介入した事実を知ったり、重大な過失により知らないでその営業秘密を使用又は公開する行為
- 二. 契約関係などによって、営業秘密を秘密として保持しなければならない義務がある者が、不正な利益を得たり、その営業秘密の保有者に損害を加える目的でその営業秘密を使用又は公開する行為
- ホ. 営業秘密が二目により公開された事実又はそのような公開行為が介入した事実を知ったり、重大な過失により知らないでその営業秘密を取得する行為又はその取得した営業秘密を使用又は公開する行為
- ヘ. 営業秘密を取得した後に、その営業秘密が二目により公開された事実又はそのような公開行為が介入した事実を知ったり、重大な過失により知らないでその営業秘密を使用又は公開する行為又は

一方、営業秘密に関する取引の安全性を確保するため、第13条では、営業秘密を取得する際に、その営業秘密が不正に公開されたこと、又は営業秘密の不正取得行為や不正公開行為が介入した事実を重大な過失なく知らずにその営業秘密を取得した善意者については、処罰の対象から除外する特例規定を設けている。

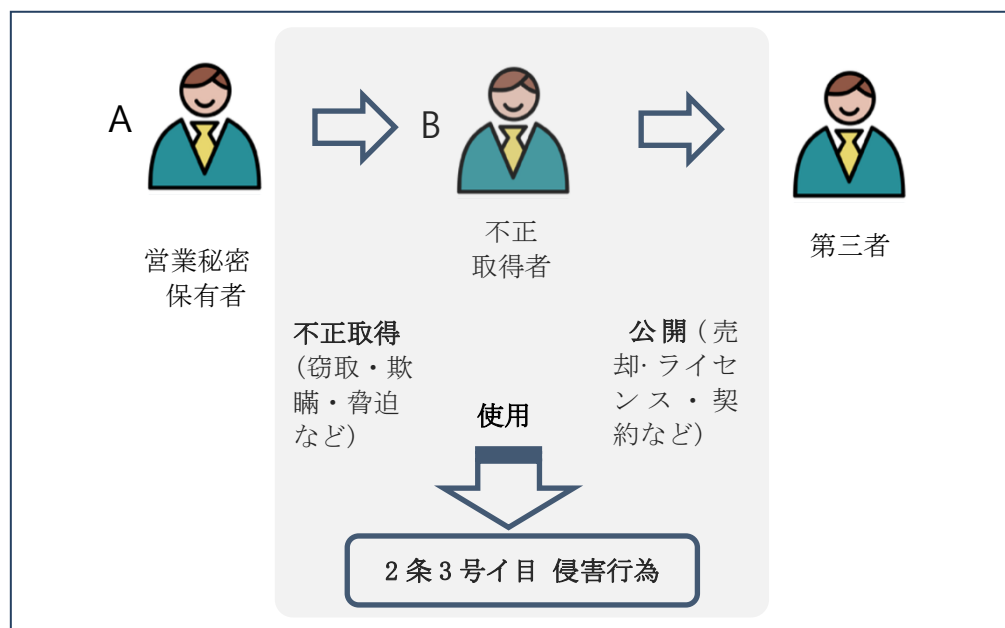
＜営業秘密侵害行為の類型＞⁵



2. 不正取得行為

窃取、欺瞞、脅迫、その他の不正な手段で営業秘密を取得する行為(以下「不正取得行為」という。)又は、その取得した営業秘密を使用又は公開(秘密を保持して特定人に教えることを含む。以下同じ)する行為(法第2条第3号イ目)

⁵ ユン・ソンヒ、キム・ジョン、チョ・ヨンスン、営業秘密保護法、法文社、p139



ここで、「窃取、欺瞞、脅迫、その他の不正な手段」などは、典型的な産業スパイ行為であって、ここで規定した「窃取、欺瞞、脅迫」は、不正取得行為の典型的な手段を例示したものであり、決してこの限りではない。

「取得」行為とは、不正な手段で営業秘密に該当する情報を得ることをいうため、正当な手段によってある情報を取得するのは、営業秘密侵害行為ではない。

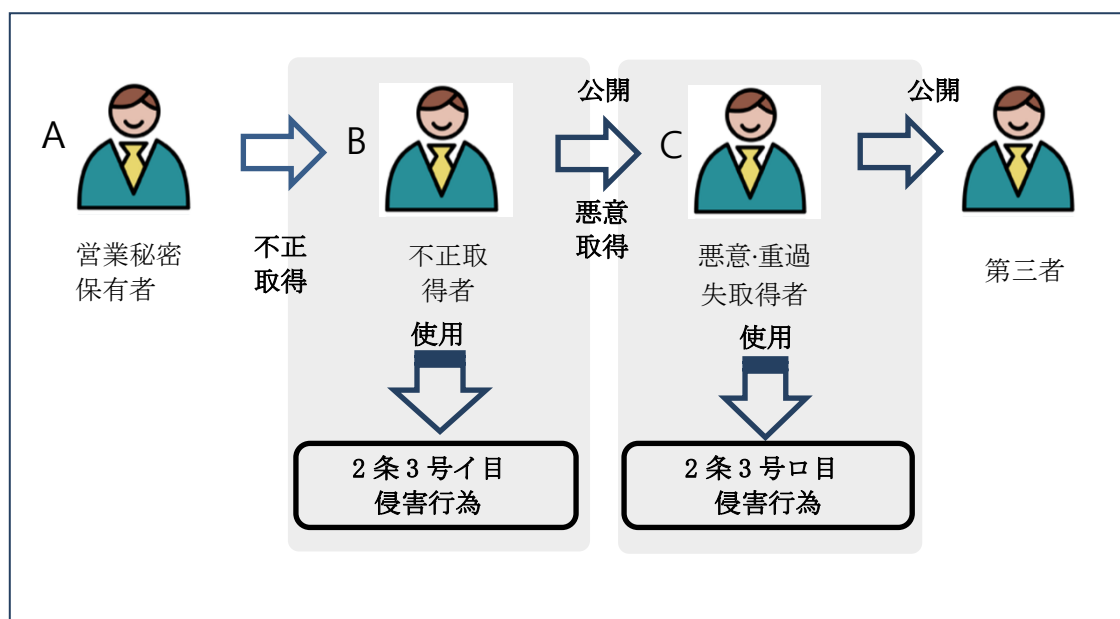
「使用」行為とは、不正な手段で取得した営業秘密を使用する行為であって、伝統的な製造・販売などに使用する行為はもちろん、必ずしも使用による利潤を上げる必要もなく、性質上、使用行為には制限がない。

「公開」行為とは、不正な手段で取得した営業秘密を特定又は不特定の人に知らせる行為をいい、秘密を保持して特定人に知らせる行為を含み、具体的態様としては、不正取得した営業秘密を第三者に売却又はライセンス契約などの方法で公開する場合などである。

本規定の不正取得・使用・公開行為の主体は、営業秘密を直接侵害した行為者であって、同行為者から転得した者は、同目の規定に該当せず、法第2条第3号ロ目又はハ目の規定に該当する。

3. 不正取得者からの悪意取得行為

営業秘密に対し不正取得行為が介入した事実を知る、又は、重大な過失により知らないでその営業秘密を取得する行為又はその取得した営業秘密を使用又は公開する行為（法第2条第3号ロ目）



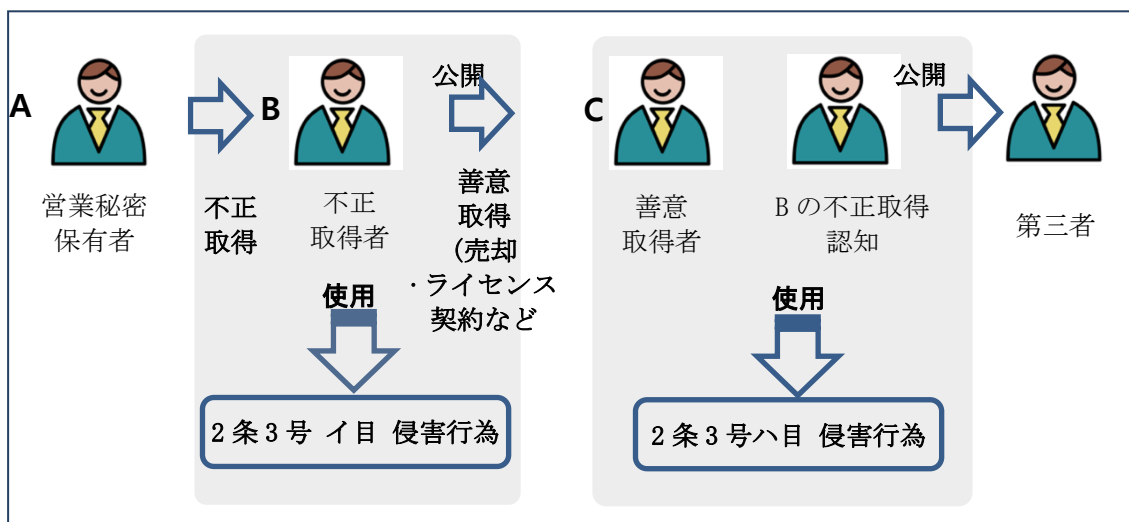
本規定の趣旨は、「イ」目の営業秘密不正取得行為後、当該営業秘密の流通過程で悪意又は重過失により当該営業秘密を転得する行為を禁止しようとする規定であって、不正取得者から直接取得した者(転得者)だけでなく、転得者から営業秘密を取得した者も本規定の適用を受ける。

同目に規定された侵害行為は、取得・使用・公開する行為であり、侵害主体は不正取得営業秘密の流通過程における全ての転得者であり、行為の判断時点は取得・使用・公開行為の当時である。

したがって、このような点から「ハ」目の事後的悪意者に対する営業秘密侵害行為が、営業秘密の取得当時には善意・無過失であったが、取得後、使用・公開時に悪意又は重過失に転換されることと区別される。

4. 事後的関与行為

営業秘密を取得した後に、その営業秘密に対し不正取得行為が介入した事実を知ったり、重大な過失により知らないでその営業秘密を使用又は公開する行為(法第2条第3号ハ目)

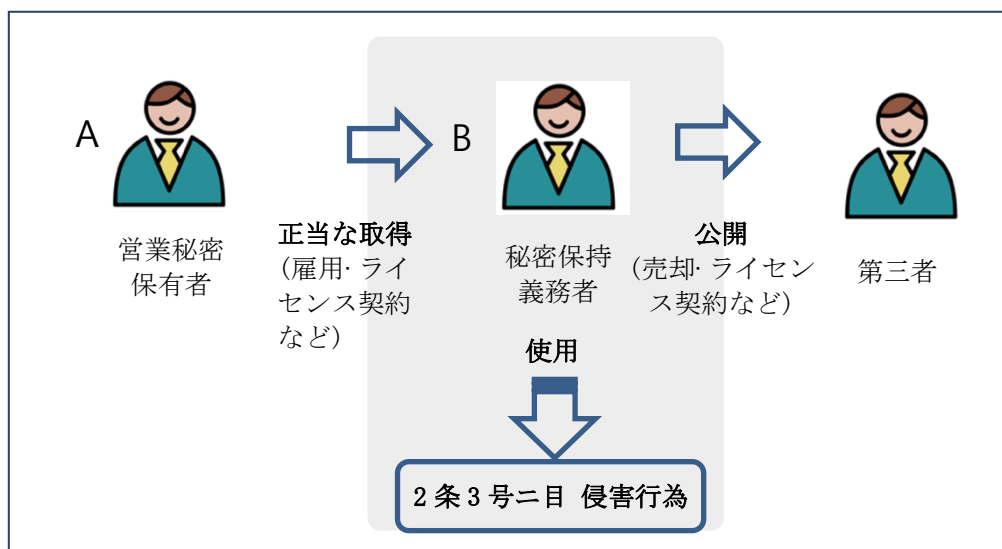


善意であり、重大な過失なしに営業秘密を取得した者が、その後営業秘密の保有者から警告を受け、又は不正な取得事実を言論を通じて知るようになるなど、自身が取得した営業秘密に不正取得行為が介入したのを知って、又は、重大な過失により知らないでこれを使用又は公開するなどの行為を規制するためのものであって、営業秘密がたとえ流出したとしても、それが秘密として保持されている間は保護する価値があるためである。

したがって、本規定は、営業秘密の取得時には善意・無過失だったが、取得後に営業秘密の保有者の通知などによって悪意又は重過失に転換される事後的悪意者の使用又は公開行為を制限しようとする規定であり、一定の要件下で営業秘密保護法第13条の「善意者に関する特例」が適用される。

5. 不正公開行為

契約関係などによって、営業秘密を秘密として保持しなければならない義務がある者が、不正な利益を得たり、その営業秘密の保有者に損害を加える目的でその営業秘密を使用又は公開する行為(法第2条第3号二目)。

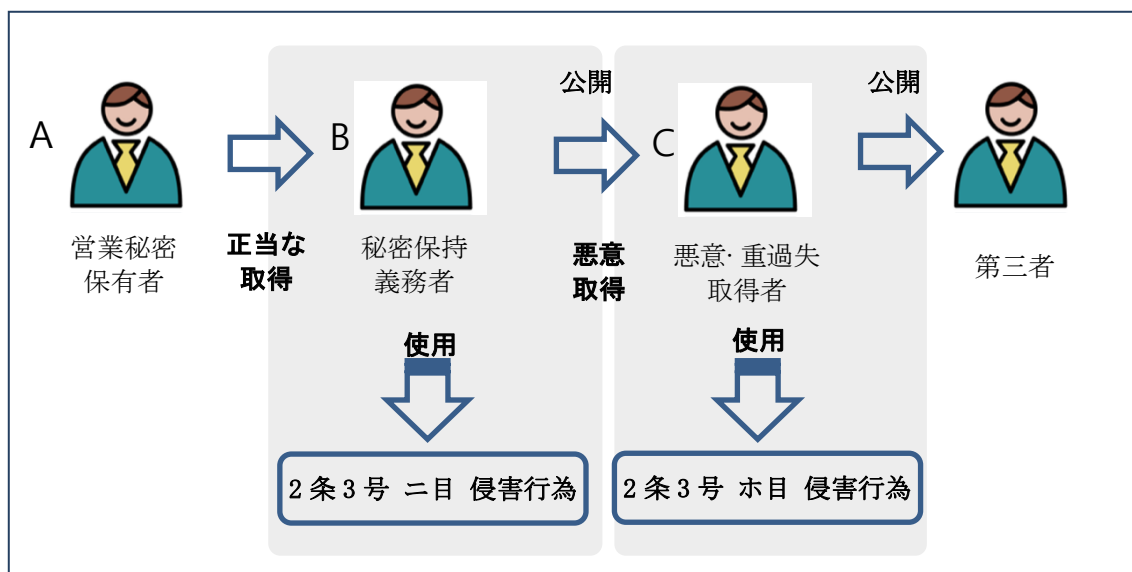


本規定は、正当に営業秘密を取得した者が秘密保持義務があるにもかかわらず、不正な目的によってこの義務を違反し、当該情報を使用又は公開する行為を規制するために設けられた。

ここで、「契約関係など」とは、必ずしも契約などのような一定の要式によってのみ発生するのではなく、使用者と従業員間又は営業秘密の保有者と実施権者間の信義関係によっても発生し、双方間の契約だけでなく、一方的な誓約書又は多数者を対象とする普遍取引約款、規則、仕様書などの形でも生じ、「秘密保持義務がある者」とは、企業体の役・職員又は営業秘密実施契約 (license) による実施権者などがこれに該当する。

6. 不正公開行為者からの悪意取得行為

営業秘密が、二目により公開された事実又はそのような公開行為が介入した事実を知ったり、重大な過失により知らないでその営業秘密を取得する行為又はその取得した営業秘密を使用又は公開する行為 (法第2条第3号ホ目)



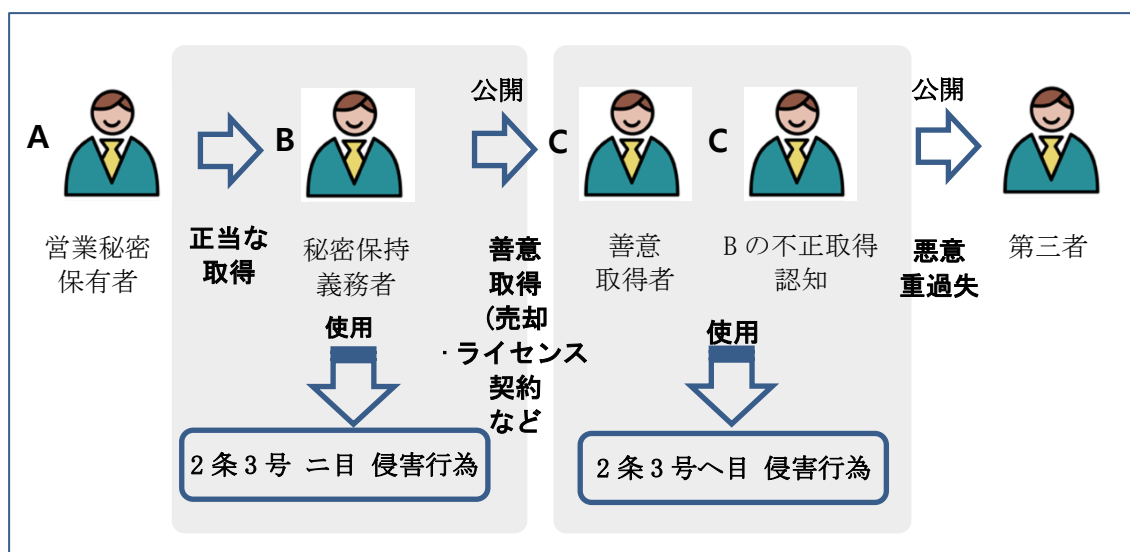
本規定の趣旨は、「二」目による秘密保持義務の違反者の営業秘密公開後、その流通過程において悪意又は重過失によって当該営業秘密を取得したり、取得した営業秘密を使用又は公開する行為を禁止させようとする規定であり、具体的な内容は「第2条第3号ロ目」と同一である。

したがって、営業秘密の転得者が原営業秘密の保有者に対し不正行為又は損害を加える目的がなくても、営業秘密侵害行為に該当し得る。

7. 不正公開行為に関する事後的関与行為

営業秘密を取得した後に、その営業秘密が二目により公開された事実又はそのような公開行為が介入した事実を知ったり、重大な過失により知らないでその営業秘密を使用又は公開する行為(法第2条第3号へ目)

本規定は、営業秘密の取得時には善意・無過失であったが、営業秘密の保有者の通知などによって悪意・重過失に転換して処罰する規定であり、具体的な内容は「第2条第3号ハ目」と同一である。本規定については、一定の要件下で「善意者に関する特例」が適用される。



8. 営業秘密保護法第2条第1号ヌ目の不正競争行為

営業秘密保護法第2条第1号ヌ目は「その他に他人の相当な投資や努力によって得られた成果などを公正な商取引慣行や競争秩序に反する方法で自己の営業のために無断で使用することによって他人の経済的利益を侵害する行為」を不正競争行為の一つの類型として定めている。

一方、営業秘密侵害行為について、第2条第3号各目と同様に独自規定として見て、第2条第1号ヌ目を適用できるのか、それとも第2条第3号各目に該当しない場合に例外的かつ補充的にのみ適用できるのかについては議論がある。

これに対して、学界と判例の態度は、第2条第1号ヌ目の一般規定としての性格上、関連法規条項の個別的構成要件の充足が困難であるため、その適用が困難であるときのみ補充的に適用される補充的な一般規定とみなすべきである⁶というのが一般的である。

また、不正競争行為民事事件のうち、権利者がヌ目とともに他の類型の不正競争行為を主張した場合において、ヌ目とともに他の類型の不正競争行為が認められたり、ヌ目だけが認められた場合より、ヌ目だけが棄却された事件の方が多い。これは法院が、「ヌ目」を補充的規定として見なして、その適用範囲を制限的に解釈しているためと考えられる⁷。したがって、営業秘密侵害行為について民事・刑事措置をとるに当たっては、第2条第1号ヌ目を第2条第3号各目とともに主張することが望ましいと思われる。ただし、未だ第2条第1号ヌ目の適用要件に関する大法院の判決がないだけに、今後の大法院の判断を見守る必要がある。

⁶ パク・ジョンヒ、「不正競争防止法第2条第1号ヌ目の適用範囲」、特許法院開院20周年記念論文集(2018)、831;特許法院 2017.9.1. 宣告2017ナ1568判決(確定)

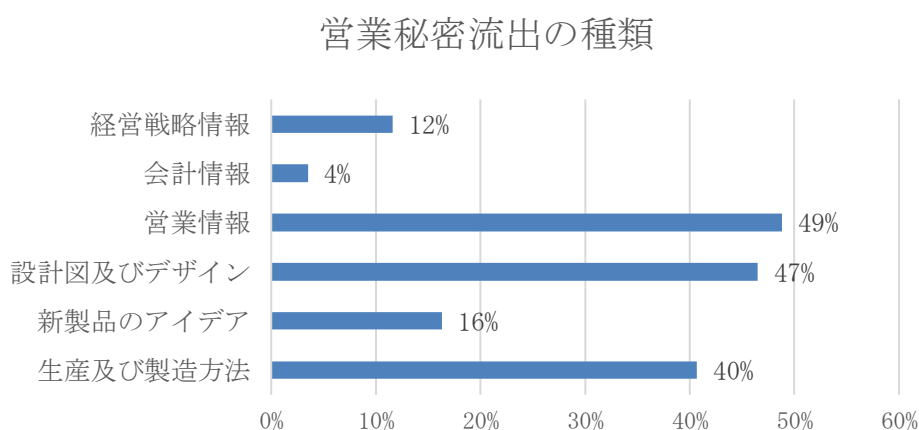
⁷ 不正競争防止法に関する国内判決文の分析研究、特許庁産業財産保護政策課、p45

第 3 章 営業秘密保護法における営業秘密侵害行為類型の事例

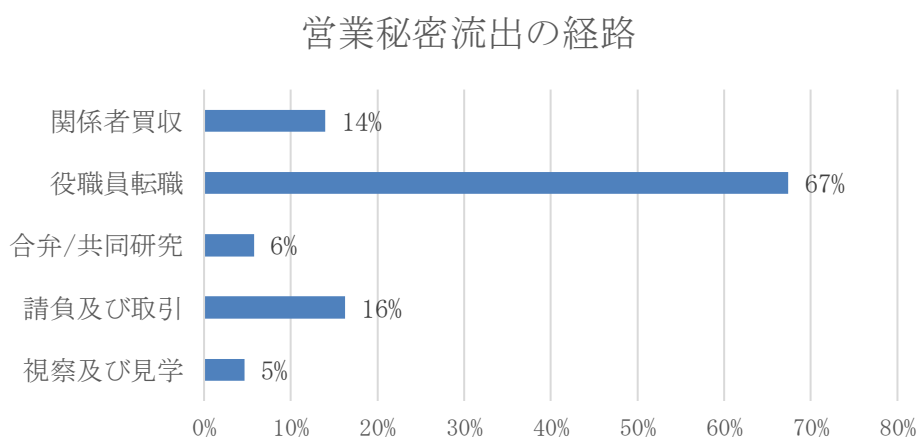
1. 営業秘密の侵害類型別統計

特許庁が行った2016年度の韓国企業の国内外における営業秘密被侵害実態調査⁸の結果は、以下のとおりである。

まず、営業秘密流出の種類を見ると、営業情報(顧客及び取引先情報)が最も高く、次に開発製品、あるいは設備の設計図及びデザインと生産製造方法(混合比等)の順であることが分かった。



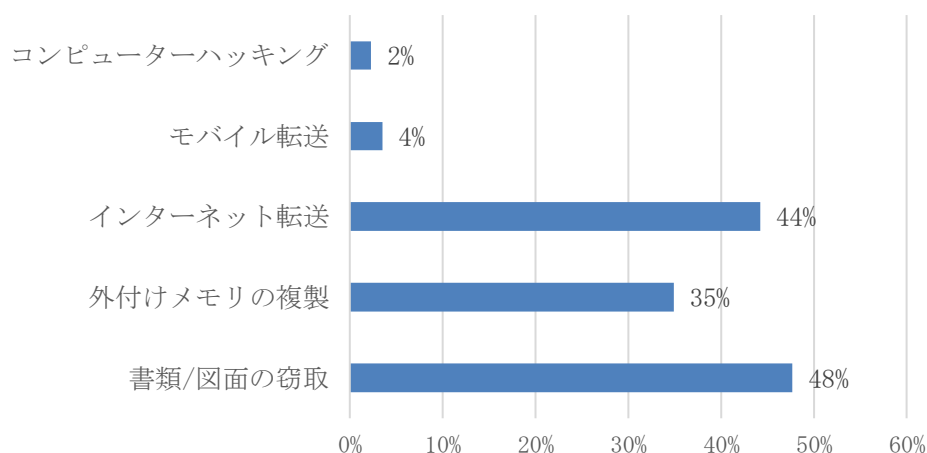
また、営業秘密の流出経路を見ると、在職中又は退職した役職員が競合他社に就職する過程での流出が最も高いことが分かった。



⁸ 2016年度韓国企業の国内外営業秘密被侵害実態調査、特許庁韓国知的財産研究院

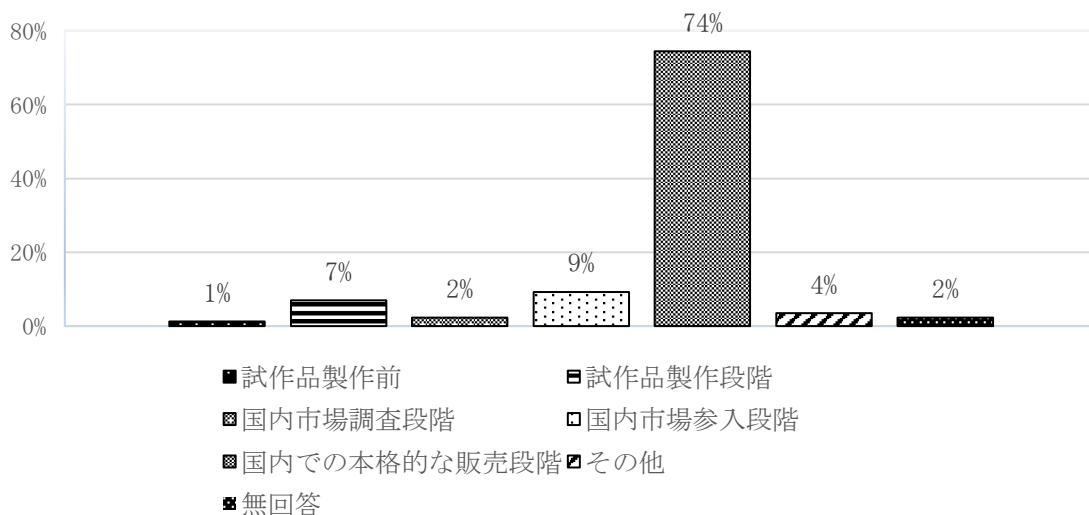
また、営業秘密流出の方法を見ると、書類、図面の窃取が最も多く、電子メール等を利用したインターネット転送による流出が続ぎ、コンピュータハッキングを利用した流出が最も低かった。

営業秘密流出の方法



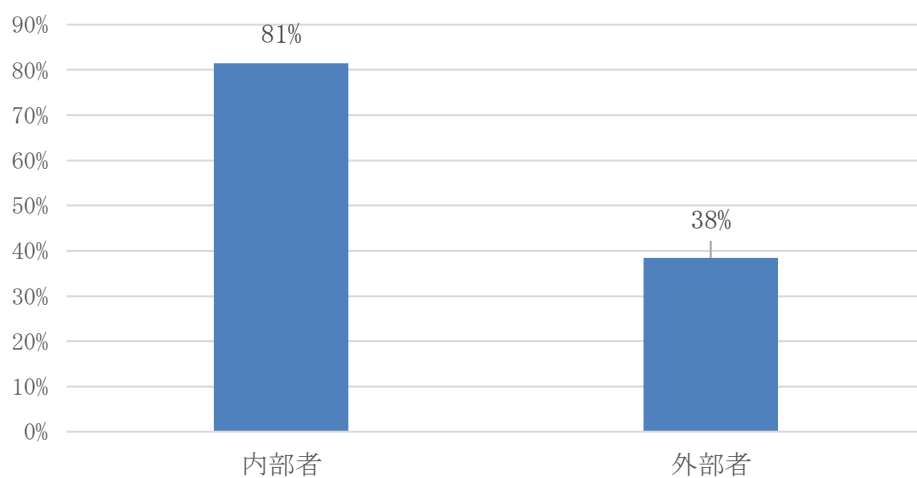
営業秘密流出の時点を見ると、国内で本格的な販売が始まる段階での流出が最も多かった。ただし、企業規模別に詳細データを見ると、大企業の製品企画段階での流出が相対的に多く、中堅及び中小企業の場合、市場参入時点での流出が相対的に多かった。

営業秘密流出時点



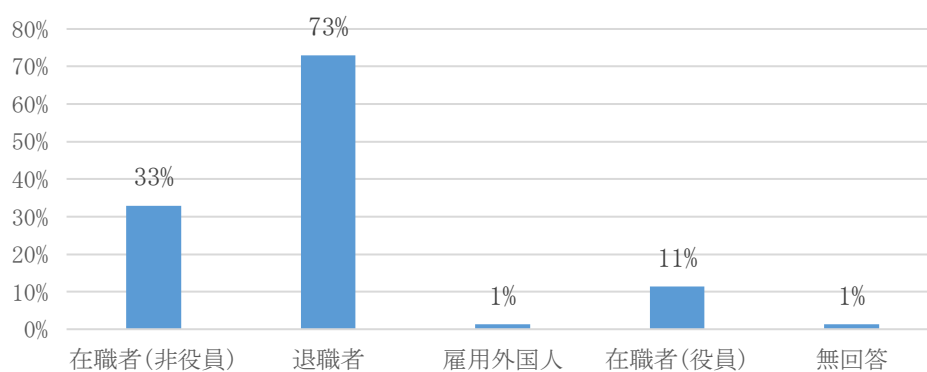
次に流出主体を見ると、複数回答を許容した際、内部者と回答した割合が外部者と回答した割合より2倍以上高かった。

営業秘密流出の主体

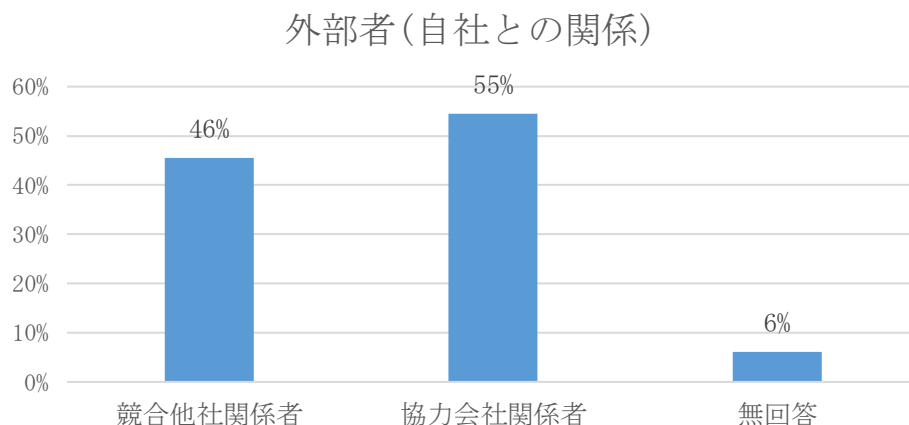


また、流出主体が内部者である場合、自社との関係において、退職者の割合が圧倒的に高く、次に非役員である在職者の順に高かった。

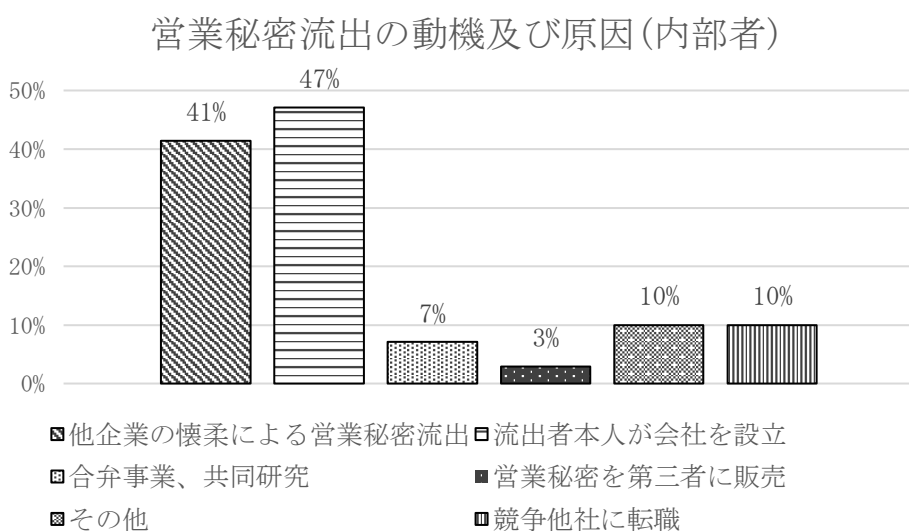
内部者(自社との関係)



そして、流出者が外部者である場合、自社との関係において、競合他社関係者の場合より、協力会社関係者の場合の方が高かった。



また、流出者が内部者である場合、流出者自身が本人の会社を設立するための目的が最も多く、次いで他社の懐柔によるものが多かった。



2. 不正取得行為

2.1 Lグループ系列会社、ATMコアプログラム不正取得摘発事例⁹

＜事件の概要＞

中小協力会社から現金自動入出金機(ATM)のコアプログラムを盗み出した後、変形させて同種のプログラムを作成して営業した嫌疑(営業秘密保護法違反)で、Lグループ系列会社のP代表などが不拘束立件された事件。

⁹ 京郷新聞、2012. 12. 3

<事件の背景>

Lグループ系列会社は、コンビニやスーパー、高速道路のサービスエリアなどにATM機を設置・運営しており、中小協力会社のA社からATM機の運営プログラムと維持保守サービスを受けてきた。

<流出の経路>

P代表などは年間25億～30億ウォンのATM機の維持・保守費用を節減するために、A社に2010年から数回にかけてプログラムのソース公開を要求したが、A社がこれを拒否した。そこで、部下の職員に指示して、A社所属の派遣職員のノートパソコンに保存されていた金融自動化機器プログラムのソースを移動式保存装置(USB)を利用してこっそりと盗み出した後、これを使用した嫌疑を受けている。

<営業秘密の流用及び予想被害>

Lグループ系列会社は、去る6月の入札では最初からプログラムソースを公開する条件で入札資格を制限してA社が脱落するようにした後、盗み出したソースを利用した変形プログラムで引き続き営業をしてきており、プログラムの流出によるA社の予想被害額は開発費と期待収益を合わせて74億ウォン余りに達すると推定される。

2.2 競合他社に転職して営業秘密を盗み出した職員の摘発事例¹⁰**<事件の概要>**

競合他社に転職し前職の業務上の秘密を盗み出した嫌疑(営業秘密保護法違反)で、従業員が拘束起訴された事件

<事件の背景>

ファイナンシャル会社であるW社は、自動車関連のリース事業を始めてHキャピタル所属の職員であるP氏などに転職を提案する。

<流出の経路>

W社はHキャピタル所属のP氏に転職を提案して、H社の営業秘密である顧客相談、保険見積もり、審査、管理などを含むキャプチャー画面を入手することを要請。

P氏らはW社に転職した後、Hキャピタルの在職中に得た情報を利用してHキャピタルの自動車整備システムにログインして、H社の自動車整備システム画面80件余りをキャプチャーする手法で情報を流出した。

3. 不正取得行為及び不正取得者からの悪意取得行為

¹⁰ ファイナンシャルニュース、2011.9.14

3.1 前職のメールサーバーに侵入し、営業機密を盗み出した元職員の摘発事例

11

〈事件の概要〉

過去に自身が勤務していた会社のメールサーバーに侵入し、営業機密を盗み出した嫌疑(営業秘密保護法違反)で、元職員のP氏が拘束された事件。

〈流出の経路〉

8ヶ月ほど勤務していた密陽市所在の船舶機械会社A社の管理者パスワードを利用して、自宅でEメールサーバーに侵入し、会計資料、契約書、溶接装備の中核技術図面など重要な機密を盗み出した後、同社で同僚であり、外資系会社に転職したQ氏にEメールで送った。

3.2 エアツール技術を海外に流出した元職員の摘発事例¹²

〈事件の概要〉

空気圧縮方式のエアツール工具製作技術を海外に流出した嫌疑(営業秘密保護法違反)で、元職員のP氏(39)ら3人を不拘束立件した事件。

〈流出の経路〉

慶南のある工具会社で研究開発チーム長として勤務していたQ氏が、中国・北京で機械工具会社を運営する友人R氏のスカウトを受けて退職し、エアツールの関連技術をメモリーカードに保存して流出。

〈営業秘密の流用及び予想被害〉

Q氏は技術を渡した代価として、友人R氏の中国工場で工場長として勤務していたが、R氏との対立により退職した後、国内に同種業企業を設立、類似製品を作り市場に販売し、5億ウォン相当の不当利得を得た嫌疑を受けている。

Q氏が盗み出したエアツール工具製作技術は、被害企業が15年間で45億ウォンを投資して開発した新技術で、流出時に150億ウォンほどの被害が予想される

3.3 半導体の製造技術を盗み出した研究員の摘発事例¹³

〈事件の概要〉

半導体生産工程の中核技術を盗み出した嫌疑(営業秘密保護法違反)で、釜山にあるT社の前首席研究員P氏を拘束した事件。

¹¹ 聯合ニュース、2011. 10. 25

¹² 聯合ニュース、2011. 10. 24

¹³ 聯合ニュース、2011. 7. 28

<流出の経路>

P氏は、T社の競合他社であるI社の専務取締役Q氏の年俸の2倍と住宅提供を条件とするスカウトを受け、T社を退職する際、半導体生産工程製造技術(IGS)を外付けHDDに保存して流出した嫌疑を受けた。

<営業秘密の流用及び予想被害>

流出した技術は、T社で8年間で60億ウォン余りをかけて開発したもので、半導体生産工程時に安定してガスを供給する装置であり、T社は該当技術をもとに国内有名半導体メーカーに関連部品を納品していた。

P氏の拘束当時、I社はP氏が流出した技術をもとに試作品まで生産し、半導体部品展示会に出品して、販売ネットワークの確保を始めた状態であった。

4. 不正公開行為

4.1 S社のアモレッド技術流出の摘発事例¹⁴

<事件の概要>

S社の大型アモレッドTV製造技術を競合他社であるA社に提供した嫌疑(産業技術の流出防止及び保護に関する法律違反など)で、元首席研究員だったP氏が拘束された事件。

<流出の経路>

P氏は、S社の首席研究員だった2010年8月、A社の人事チーム長とヘッドハンティング会社の職員に会い、‘大型アモレッドのTV技術である大型アモレッドTV用の技術であるSmall Mask Scanning(SMS)の開発’に参加した研究員5人とともに転職すれば、役員級の待遇をするという約束をされ、同年11月退職、1億9千万ウォンを受け取りA社に関連技術など秘密資料を提供した嫌疑を受けている。

Q氏など研究員2人は、S社の大型アモレッドのTV開発業務を遂行しながら、進捗状況などをEメールや携帯電話のメッセージ等を通してA社に転職した研究員に伝達するなど秘密を漏えいした嫌疑を受けている。

A社役員R氏(50)など5人は、S社の前・現職研究員を組織的に迎え入れ、中核技術を盗み出した嫌疑を受けている。

<営業秘密の流用及び予想被害>

90兆ウォン台の大型アモレッドTV市場を先に獲得するために、国内企業間で技術を流出した事件で、中国に流出していれば莫大な国家的損失が発生する可能性が高かった。

¹⁴ 仁川日報、2012. 4. 6

4.2 中小企業の新技术を米国に流出しようとした技術ドクターの摘発事例¹⁵

〈事件の概要〉

中小企業が開発した新技术を米国に流出しようとした嫌疑(営業秘密保護法違反)で、該当企業の技術ドクターQ氏が不拘束立件された事件。

〈事件の背景〉

技術ドクター事業は、政府出資研究機関と大学、産学協力団などの研究所員が、サポートが必要な中小企業に技術専門家として派遣され、問題解決をサポートする事業であって、京畿道が運営している。

Q氏は機械部品洗浄器の開発会社であるA社に‘技術ドクター’として勤めながら、同社が開発したエコ機械部品の洗浄技術を2009年11月米国の環境会社に2億4000万ウォンで売却をしようとした。

〈流出の経路〉

Q氏はA社に米国環境庁の安全検査承認を受けさせるという名目で、A社から関連営業秘密の資料を入手する。

〈営業秘密の流用及び予想被害〉

Q氏は流出した資料で技術売却とともに、米国で自身の名義で特許を受けようと試みたが、A社のエコ機械部品の洗浄技術が米国環境庁の安全検査承認を受けることができず、技術売却と特許出願に失敗した。

4.3 待遇への不満から競合他社に転職し、営業秘密を盗み出した職員の摘発事例¹⁶

〈事件の概要〉

年俸交渉に失敗し、競合他社に転職して営業秘密を盗み出した嫌疑(営業秘密保護法違反)で、前職員であるP氏が不拘束立件された事件。

〈事件の背景〉

IT企業で技術支援部課長として勤めていたP氏は、会社に年俸4000万ウォンを要求したが、2900万ウォンでの決定に不満を抱き、競合他社のサービスチーム課長に転職する。

〈流出の経路〉

P氏は会社のセキュリティーサーバーから見積書や契約書などファイル11700個を内密に外付けHDDにダウンロードして盗み出す。

¹⁵ ファイナンシャルニュース、2011. 11. 2

¹⁶ 聯合ニュース、2011. 10. 18

4.4 投資を口実として200億ウォン相当の技術を海外に流出した元代表らの摘発事例¹⁷

＜事件の概要＞

役員として在職していた会社の製造技術を内密に盗み出して台湾の関連業者に流出した嫌疑(営業秘密保護法違反など)で、G社代表Q氏(49)ら3人が不拘束立件された事件。

＜事件の背景＞

Q氏らは、2009年末に低密度ポリウレタンフォーム製造会社であるD社代表と対立すると、技術を盗み出すことを決心し、D社の製品に関心を見せてきた台湾のG社に先に投資を要請する。

＜流出の経路＞

D社の製品に関心を見せてきた台湾のG社の投資が確実視されると、Q氏らは‘低密度ポリウレタンフォーム’の製造に関する装備設計図などの生産技術をUSB、EメールなどでG社に流出した嫌疑を受けている。

＜営業秘密の流用及び予想被害＞

Q氏らは、G社に営業秘密を渡した代価として300万ドルの投資を受け、国内に工場を設立し同一製品を生産し、D社に215億ウォン相当の被害を与えた嫌疑を受けている。

5. 不正公開行為及び不正公開行為者からの悪意取得行為

5.1 生産設備模倣A社幹部の摘発事例¹⁸

＜事件の概要＞

競合他社から不正流出した設計図で製作された生産設備の納品を受けて使用した嫌疑(営業秘密保護法違反)で、繊維会社A社の幹部Q氏が不拘束起訴された事件。

＜事件の背景＞

P代表は、過去にH社に連続反応式重合機などの生産設備を納品していた会社に在職してから退職後、独立してS社を設立する。

＜流出経路＞

P代表は、H社が独自開発したスパンデックスの原糸生産設備である「連続反応式重合機」の設計図を過去共に勤務していた同僚を通じて入手する。

繊維会社A社の幹部Q氏は、P代表のS社から当該流出技術と類似の製品4台の納品を受け、使用する。

技術流出の主体はP代表だが、Q氏の場合、P代表の設計図の流出事実をあらかじめ知

¹⁷ 文化日報、2011. 4. 1

¹⁸ 聯合ニュース、2011. 6. 1

っていたという点が認められ、検察に起訴される。

5.2 販売権要求の拒絶を受け次世代消火器技術を流出した前職員の摘発事例¹⁹

＜事件の概要＞

自身が勤務していた会社の固体エアゾール消火器関連技術を盗み出した嫌疑（営業秘密保護法違反）で、釜山のG社の前設計課長R氏及びR氏が盗み出した技術で同種製品の生産を試みたD社代表などが拘束された事件。

＜事件の背景＞

G社の設計課長R氏は、G社の4年間の投資で固体エアゾールの開発に成功した後、2009年に1年間で32億ウォンの売上を得て、会社側に慶北地域での販売権を要求したが拒絶された。

＜営業秘密の流用及び予想被害＞

これに対し不満を抱いたR氏はG社を退職し、次世代消火器技術である固体エアゾール関連技術を盗み出し、D社及びC社と共謀して同種製品を製造、販売を試みた嫌疑を受けている。

当該技術は、国内で初めて開発されたものであり、今後3年間で600億ウォンの売上が予想される次世代技術である。

6. 日韓間の営業秘密侵害紛争の事例

6.1 ポリプロピレン製造特許技術流出事件²⁰

＜事件の概要＞

米国の石油化学会社U社と子会社の日本のN社が、韓国のH社を相手取り営業秘密侵害の禁止及び契約違反行為の禁止を理由に訴訟を起こした事件。

＜事件の背景＞

H社はU社と1989年ポリプロピレン製造特許技術の使用を許可する契約を結ぶ。その後、H社は2013年ポリプロピレン工場増設工事を施工会社のD社に請け負わせ、ポリプロピレン製造工程の図面を提供した。これに対し、U社は「営業秘密の技術情報を工場新築に使用したことで、これは契約義務違反であり不正競争行為である」とし、2014年3月に工場の稼働中断など使用禁止と176億ウォン余りの賠償を請求した。その後、H社は自主的に工事

¹⁹ 聯合ニュース、2011. 3. 29

²⁰ 法律新聞、2019. 12. 24

を続け、2015年8月に工場を完成しプロピレンを生産している。

〈結果〉

第一審では「H社が施工会社であるD社に厳格な秘密保持義務を課した状態で設計図書を提供した以上、その過程で原告らが新たに営業秘密保護という法益を侵害されたとは考えにくい」として原告敗訴の判決を下した。

第二審では「H社が各技術情報を含む図面を施工会社に提供した行為は営業秘密の公開であって、原告らの営業秘密を侵害した行為」とし、H社に、完工した工場の稼動を中断し、5億ウォンをU社側に支払うよう言い渡した。

大法院では、当事者間で結んだエンジニアリング契約の本文により、米国イリノイ州法が準拠法となるにもかかわらず、原審は契約上の準拠法を見過ごし、何の検討もせず韓国法を適用し、工場稼動中断と損害賠償義務成立の可否を判断した誤りがあるとして原審を取り消した。

6.2 電気鋼板技術流出事件²¹

〈事件の概要〉

日本の鉄鋼メーカーN社が、韓国の鉄鋼メーカーP社を相手取り2012年4月に日本の東京地裁に営業秘密侵害禁止及び約1兆ウォンの損害賠償を請求する訴訟を起こした事件。

〈事件の背景〉

P社の電気鋼板研究部署に勤務していたLは、数回にわたり昇進が叶わなかったことに不満を抱いて退社し、技術コンサルティング会社を立ち上げた後、中国鉄鋼会社B社とコンタクトして、技術諮問の名目で50億ウォンを受け取り、電気鋼板技術を提供した。

そこで、P社は営業秘密流出の疑いでLを告訴し、Lは捜査過程において、自分たちが外部に持ち出した「電気鋼板製造技術」はP社固有の技術ではなく、P社に在職時にN社を退職した研究員たちを直接渉外して彼らから得た技術だと陳述した。

被告人のうち、退社後に鉄鋼関連会社を立ち上げ、P社の支援を受けたと主張した者もいるが、N社からリストラされた後、韓国大学の客員教授として採用され、その後P社と電気鋼板の共同研究をした者もいた。

このような捜査記述を入手したN社は、訴訟に備えて、退職した自社社員を全数調査するなど、自分たちの技術がP社に流出したことを立証する資料を蓄積した後、P社を相手どり日本と米国で同時に営業秘密侵害及び特許侵害を理由とする損害賠償訴訟(986億円)を起こした。

N社は、N社が12年で完成した技術をP社が1年半で完成したと主張しており、これに対してP社はP社独自の技術だと反論した。

²¹ 朝鮮日報、2015. 10. 17.

〈結果〉

2015年5月末、P社とN社は最終合意に至り、4ヵ月後の2015年9月30日付の公示を通じて、300億円を支払う代わりに、N社との全ての訴訟で和解したと明らかにした。

7. 新たな侵害形態

上記のように、従来韓国の判例等に見られる営業秘密の不法流出の現状の多くは、企業の内部者が関与しており、企業内部者の関与のない産業スパイの独自侵害行為はほとんどないことがわかる。

しかし、最近では企業内部者の関与なく、ランサムウェアや標的型メール攻撃といったサイバー攻撃により、企業が保有している技術情報や営業情報を奪い取る行為が新たな侵害類型として現れている。

実際にウェブホスティング会社がランサムウェアに感染し、ハッカーとの交渉の結果、13億ウォン相当のビットコインを支払った事例²²がある。ウェブホスティング会社を攻撃したハッカーたちは、当該会社が主に使用する無料OSであるLinuxサーバーにランサムウェアを流布して顧客データに関するファイルを暗号化させた後、復号を対価に金銭を要求した。

一方、標的型メール攻撃が毎年大きく増加している日本²³と異なり、まだ韓国では標的型メール攻撃に対する数値化された調査資料は見当たらないが、採用書類を偽装して企業関係者のコンピュータを感染させた事例等が報告²⁴されている。

²² URL:<http://www.yonhapnews.co.kr/bulletin/2017/06/15/0200000000AKR20170615125100017.HTML?input=1179m> (聯合ニュース、2017. 6. 15、最終アクセス2018. 7. 21)

²³ 警察庁報道発表資料、前掲注(48)、p1・p4; 経済産業省、前掲注(3)、p78

²⁴ URL:<http://www.ebn.co.kr/news/view/886277> (EBNニュース、2017. 4. 11、最終アクセス2018. 7. 18)

第 4 章 営業秘密保護のためのその他の制度

1. 技術資料任置制度

技術資料任置制度は、委託取引上、優越的地位にある大企業による不当なコア技術の提供要求から中小企業の技術を保護するための制度である。

技術資料任置制度では、中小企業自ら自己の技術を安全な第三者機関に委託する一方、破産など特定の交付要件が発生した場合に使用機関である大企業が第三者機関からその技術の交付を受けて使用できるようにしている。

これにより、中小企業は大企業に技術資料を公開する必要がなく、営業秘密を安全に保護でき、また大企業も、中小企業の破産などに関係なく安全な技術の使用が保証される。

2. 下請取引の公正化に関する法律

公正取引委員会は、下請取引の公正化に関する法律(以下「下請法」という。)を改正し、技術奪取行為を不公正行為として禁止している(第12条の3)。

改正下請法によれば、下請関係にある親事業者の下請事業者に対する不当な技術資料の要求を禁止しており、これに違反した場合、親事業者に罰則、罰金、損害賠償などを課するよう規定(第30条、第35条など)している。

なお、新しく2021年7月23日に国会を通過した改正法では、以下のとおり下請法を改正して、下請事業者の技術を手厚く保護するとともに、損害賠償訴訟時の被害事業者の資料確保の困難性を解消している。

[表6]

	改正前	改正後
技術資料の要件緩和	合理的努力によって秘密として保持された資料(第2条第15項)	秘密として管理される資料
秘密保持契約の義務化	-	下請事業者が親事業者に技術資料を提供する場合、親事業者が下請事業者と技術資料について秘密保持契約を締結するよう義務化(第12条の3第3項)
法院の資料提出命令制の導入	-	損害の証明又は損害額の算定に必要な場合、営業秘密に該当しても、法院が資料提出を命じることができるようにする(第35条の2～第35条の5)

3. 営業秘密原本証明制度

営業秘密侵害訴訟において、営業秘密の存在及び保有事実を立証することが容易でないという点を考慮して、特許庁傘下の営業秘密保有センターでは営業秘密原本証明制度を運営している。

営業秘密原本証明サービスは、「タイムスタンプ」という電子的技術を用いて電子文書の生成時点及び原本であるか否かについて第三者機関が証明し、当該電子文書自体は作成者が保有するという仕組みである。

営業秘密原本証明サービスを活用する場合は、以後当該電子文書が流出した場合に、営業秘密侵害に関する訴訟において、当該電子文書に収録された営業秘密の存在有無、存在時点及び保有有無に対する営業秘密保有者の立証責任が緩和される(営業秘密保護法第9条の2)。

4. 産業技術の流出防止及び保護に関する法律

従来、営業秘密保護法が、企業ではない政府の研究所や大学の先端技術の海外不法流出に弱いという問題点を認識して、2006年10月27日『産業技術の流出防止及び保護に関する法律』(以下「産業技術保護法」という。)が制定された。

営業秘密保護法上の保護対象である営業秘密は、技術上の情報と経営上の情報を全て含む概念であるが、産業技術保護法における保護対象は「産業技術」及び「国家コア技術」に限定されている。

一方、2015年改正法では、保護対象となる産業技術の範囲が不明確であるという指摘により、同法によって保護される産業技術の範囲に、国家コア技術(第2条第1号イ目)、建設新技術(第2条第1号ヘ目)、保健新技術(第2条第1号ト目)及びコア基幹技術(第2条第1号チ目)が含まれることを明示的に規定し、その他の法令により指定告示公告認定される技術の場合、産業通商資源部長官が官報に告示する技術のみ産業技術の範囲に含まれるようにした。

また、2016年改正法の産業技術保護法では、産業技術の海外流出行為に対しては15年以下の懲役又は15億ウォン以下の罰金に処し(第36条第1項)、国内流出行為については7年以下の懲役又は7億ウォン以下の罰金に処するようにして(第36条第2項)、量刑基準を強化した。

さらに、営業秘密保護法と異なり、産業技術保護法では、産業技術の流出により得られた財産上の利益を没収できるようにする一方、没収が困難な場合はその価額を追徴するようにしている(第36条第4項)。

5. 防衛産業技術保護法

防衛産業に関する不法な技術流出の問題を防ぐため、防衛産業技術を体系的に保護し、不法な流出を防ぐため、2015年12月29日に防衛産業技術保護法が制定された。

前述の産業技術保護法と防衛産業技術保護法は、目的、対象機関、保護技術、刑事処罰等について、以下のような違いがある。防衛産業技術保護法は産業技術保護法に比べ刑事処罰が強いが、民事救済手段としての侵害禁止権を規定しておらず、紛争解決に関わる規定も導入されていない。

[表7]

	産業技術保護法	防衛産業技術保護法
目的	● 産業技術の不正流出防止 ● 国家コア技術の保護	● 防衛産業技術の体系的保護、国家安全保障 ● 国家信頼度の向上
対象機関	産業技術を保有する企業、研究機関、大学	防衛産業技術を保有、又は防衛産業技術に関する研究開発事業を遂行している機関
保護技術	産業技術及び国家コア技術 (中央行政機関の長の指定及び告示)	防衛産業技術 (防衛事業庁長の指定及び告示)
刑事処罰	● 海外流出:15年以下の懲役、15億ウォン以下の罰金 ● 国内流出:7年以下の懲役、7億ウォン以下の罰金	● 海外流出:20年以下の懲役、20億ウォン以下の罰金 ● 国内流出:10年以下の懲役、10億ウォン以下の罰金
民事的救済	禁止請求権	-
紛争調停	産業技術紛争調停委員会	-

6. 中小企業保護法

独自技術の保護能力が不十分であり、大企業との受・委託関係により技術流出に弱い中小企業を保護するため、2014年5月26日に中小企業技術保護支援に関する法律(以下「中小企業保護法」という。)が制定された。

中小企業保護法により保護される中小企業技術は、独立した経済的価値を有する技術又は経営上の情報であって、公然と知られておらず、秘密として管理される中小企業の技術(第2条第2号及び第3号)である。したがって、中央行政機関の長又は防衛事業庁長が指定及び告示した分野の技術である場合に保護対象として認められる産業技術や防衛産業技術とは異なり、中小企業保護法による保護を受けるためには、営業秘密保護法上の営業秘密と同様に、保有技術が非公知性、経済的有用性、秘密管理性の要件を満たさなければならないという限界がある。

一方、中小企業保護法は、中小企業のセキュリティ能力を強化するための支援法的な性格を有しており、履行命令や罰則等の規定を設けるには限界がある²⁵。

したがって、中小企業技術の侵害行為は、産業技術保護法や防衛産業技術保護法とは異なり、刑事的制裁の代わりに中小企業技術侵害行為の申告及び調査(第8条の2)、中小企業技術侵害行為に関する勧告及び公表(第8条の3)などの行政規制の対象となる。

7. 刑法

²⁵ 産業通商資源中小ベンチャー企業委員長、不正競争防止及び営業秘密保護に関する法律一部改正法律案(代案)、2018、15p

刑法では、業務上背任罪、窃盗罪、財物損壊罪、秘密侵害罪、業務妨害罪などの規定により、営業秘密の不正な流出行為を間接的な方式で規制することによって営業秘密を保護する。

実際に、営業秘密の流出に関する刑事事件のうち、企業の所属役員・従業員による営業秘密の流出事例が最も大きな比重を占めており、営業秘密侵害に関する刑事訴訟では、業務上背任罪に関する規定が営業秘密保護法と競合的に適用される場合が多い。

8. 商法

商法第382条の3では取締役の忠実義務を規定しており、第382条の4では取締役が在任中だけではなく、退任後にも職務上知り得た会社の営業上の秘密を漏えいしないよう禁止する秘密保持義務を規定している。また、商法第397条では、取締役の競業禁止義務を規定している。

このように、商法では、取締役など役員に対する営業秘密保持義務及び競業禁止義務を規定しており、前・現職役職員による営業秘密の流出の防止を図っている。

9. 知的財産基本法

知的財産の創出、保護及び活用に関する政府の各部署の法政策を総括的に指導し調整できる制度と条則を設けるために、2011年5月19日に知的財産基本法が制定、公布された。

知的財産基本法第28条では、知的財産の公正な利用秩序の確立のために、政府は大企業と中小企業間の不公正な知的財産の取引を防止し、相互間の協力を促進するよう規定している。

第 5 章 営業秘密侵害に対する法的措置及び最近の判例の動向

1. 営業秘密侵害に対する法的措置

1.1 民事上・刑事上の措置

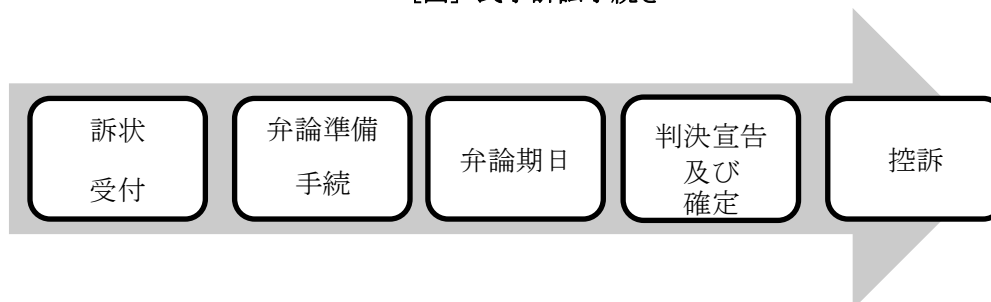
(1) 民事上の措置

(a) 概要及び手続き

営業秘密侵害の際、被害者は法院に民事訴訟を提起し、営業秘密侵害行為の禁止、侵害を構成した物の廃棄又は除去などを請求する一方、営業秘密侵害行為によって発生した損害及び信用失墜に対して原状回復を求める請求をすることができる。

また、民事訴訟の確定判決を受けるまで長期間が必要とされる点を考慮し、法院に営業秘密の侵害禁止、転職禁止などの仮処分申請を行なうこともできる。

〔図〕民事訴訟手続き



(b) 根拠法律

侵害された技術が営業秘密保護法上の営業秘密の要件を満たしている場合、営業秘密保護法第10条ないし第12条に基づき損害賠償、侵害禁止及び信用回復請求が可能である。

また、侵害された技術が産業技術保護法上の産業技術に該当する場合、産業技術保護法第14条に基づき侵害禁止を請求することができる。

(2) 刑事上の措置

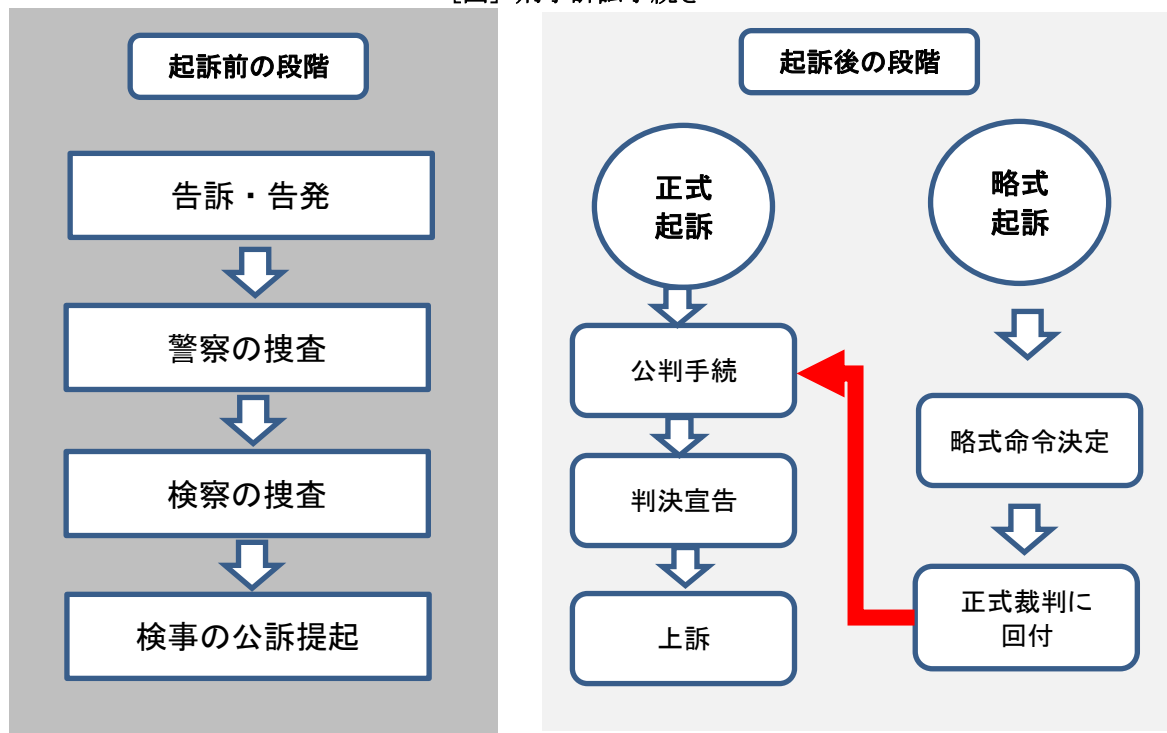
(a) 概要及び手続き

営業秘密流出における被害者は、刑事訴訟を通じて国家公権力による侵害者の処罰を要求することができ、さらに検察の捜査過程で確保した証拠を利用して後日仮処分などの民事訴訟において活用することができる。

一方、通常、刑事訴訟手続きは、当事者の告訴又は告発によって始まり、親告罪における告訴は訴訟条件に該当するため、検事の公訴提起は告訴によって左右される。しかし、営業秘密保護法違反のように非親告罪での告訴は捜査の端緒に過ぎないため、告訴の有無は検事の公訴提起に大きな影響は及ぼさない。検事の公訴提起を基準に大きく起訴前の段

階と起訴後の段階に分けられる。検事が被疑者を起訴すると決定した場合、正式裁判に付する正式起訴と、書類のみにより裁判し罰金刑として処理するよう求める略式起訴を請求することができる。

〔図〕 刑事訴訟手続き



(b) 根拠法律

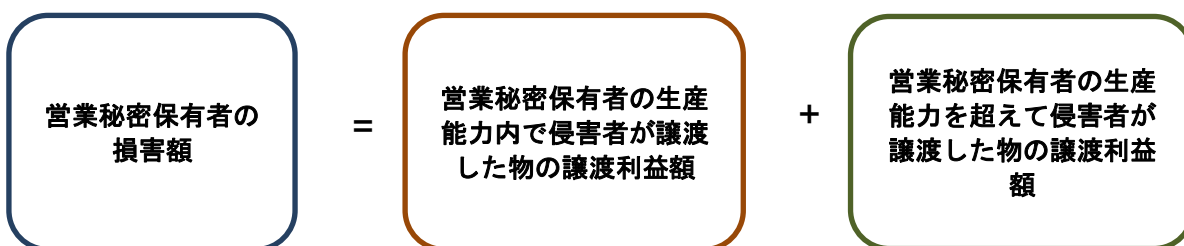
- ① 流出技術が営業秘密保護法上の営業秘密に該当する場合、第36条に基づき刑事告発が可能である。
- ② 一方、流出技術が産業技術保護法又は防衛産業技術保護法に定める産業技術又は防衛産業技術に該当する場合、特別法優先原則により当該法律が優先的に適用される。
- ③ また、流出技術が営業秘密保護法、産業技術保護法及び防衛産業技術保護法で定められている保護対象として成立しない場合でも、刑法で定められている違法行為の要件を満たす場合は、当該規定に基づき処罰が可能である。
営業秘密侵害に関して刑法上規定されている違法行為としては、業務上背任罪、窃盗罪、財物損壊罪、秘密侵害罪、業務妨害罪などがある。
- ④ 営業秘密流出の経緯が、当該営業秘密保有企業の情報通信網を侵害して行われた場合、情報通信網侵害罪が成立する可能性がある。
また、業務上背任による営業秘密侵害行為によって経済的利得や損害が甚大な場合は、加重処罰に関して特定犯罪加重処罰等に関する法律違反罪の適用可否も問題になる。

1.2 侵害賠償額の算定及び懲罰的賠償制度

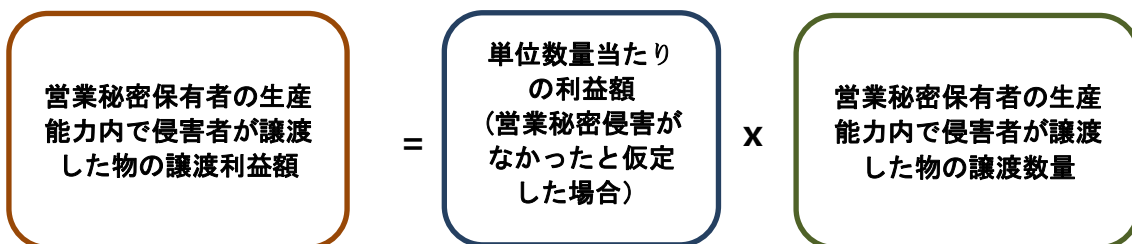
(1) 営業秘密保護法上の損害賠償額の推定規定

(a) 営業秘密を侵害して販売した物の譲渡利益額(営業秘密保護法第14条の2第1項)

2020年12月22日改正の営業秘密保護法第14条の2第1項では、営業秘密保有者の生産能力内で営業秘密を侵害して販売した物の譲渡利益額と、営業秘密保有者の生産能力を超えて侵害者が譲渡した物の譲渡利益額とを合算した額を損害額として推定するとされている。



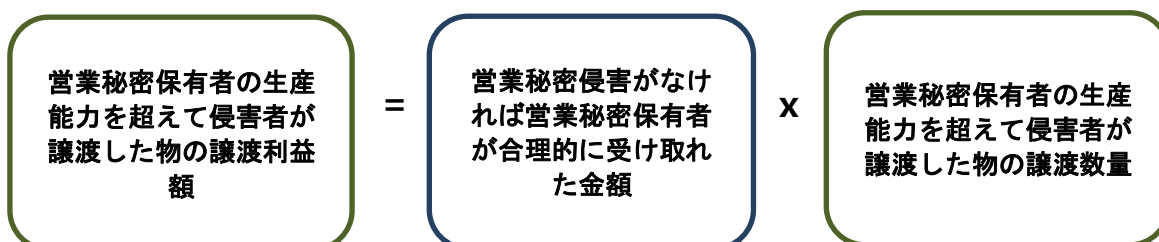
ここで、営業秘密保有者の生産能力内で侵害者が譲渡した物の譲渡数量は、営業秘密保有者が生産可能な数量から営業秘密保有者が実際販売した数量を引いた数量を超えないようにする。



従来の推定規定では、損害額の推定時に、営業上の利益を侵害された者が生産できた物の数量から実際に販売した物の数量を差し引いた数量に単位数量当たりの利益額を乗じた金額を超えないようにしていた。すなわち、営業秘密保有者の生産能力から外れた範囲については損害賠償額の算定から除外されていた。

この場合、侵害者の譲渡数量が特許権者の生産能力を超えた場合、侵害者がその超過数量分の利益を不当に受け取ることになるという問題点があった。

したがって、改正法では、営業秘密侵害者が、営業秘密保有者の生産能力を超えて譲渡した数量についても損害額算定時に含めることとした。



ここで、営業秘密保有者の生産能力を超えて侵害者が譲渡した数量とは、

- ①営業秘密侵害者が譲渡した数量のうち、営業秘密保有者の生産可能な数量から営業秘密保有者が実際に販売した数量を差し引いた数量(すなわち、営業秘密保有者の生産能力内で侵害者が譲渡した数量を超えた数量)、又は、
- ②営業秘密侵害行為以外の理由で営業秘密保有者が販売することができなかった数量を意味する。

(b) 侵害行為による利得額(営業秘密保護法第14条の2第1項)

侵害者が営業秘密侵害行為によって利益を得た合、その利益額を損害額として推定する。

判例は一貫して、営業秘密侵害時における財産上の利益額の算定基準を次のように説示している。

-判例で説示する営業秘密侵害時における財産上の利益額の意味、算定基準

被告人が営業秘密を取得することによって得た利益は、その営業秘密が有する財産価値相当、かつその財産価値はその営業秘密を用いて競合他社など他の業者で製品を作る場合、その資料によって技術開発に必要とされる費用が減少する場合のその減少分相当と、さらにその資料を利用して製品生産にまで発展させる場合、製品販売利益のうちその資料が提供されなかった場合との差額相当であって、そのような価値を勘案して市場経済原理によって形成される市場交換価格

一方、韓国大法院では、営業秘密を使用する場合に支給しなければならない技術使用料相当額、又は韓国取引技術研究所における収益接近法を用いて該当営業秘密の経済的価値を評価した評価金額については、営業秘密侵害時に得ることができる財産上の利益額と見なすことはできないと判示している。

このような韓国大法院の営業秘密侵害時における財産上の利益額の算定方法及び条件に対する姿勢を見ると、財産上の利益額を算定又は立証することは実質的にほとんど不可能といえる。

ここで侵害者の利益額を何ととらえるのかが問題になるが、実務的には当該製品を製造販売するのに要した費用を控除した純利益ととらえている。

(c) 実施料相当額(営業秘密保護法第14条の2第3項及び第4項)

営業秘密の使用によって得ることができる実施料相当額を最小限の損害と推定することができる。

実務的には、契約上他の実施例を参照するか、あるいは関連取引業界の一般的な使用料や鑑定に基づくか、あるいは取引実態に鑑みて相当だと評価される金額を実施料として算定する。

実際に実施料相当額を超えて損害が発生する場合も、その超過額を追加で請求することができ、一方、侵害者に故意又は重過失がなければ、法院は損害賠償額を算定するにあたり、これを参酌することができる(営業秘密保護法第14条の2第4項)。

(2) 法院の裁量による認定

上記のような損害額の推定規定にもかかわらず、請求権者が損害額を立証するのが容易でない場合、弁論全体の趣旨と証拠調査の結果に基づいて相当な損害額が認められる。ただし、このような場合も、損害の発生事実自体に対しては請求権者が主張・立証しなければならない。

(3) 懲罰的賠償制度の新設

2019年1月8日改正の営業秘密保護法では、悪意ある営業秘密侵害行為により営業秘密保有者の営業上の利益を侵害し損害を与えた者に対して、損害と認められた金額の3倍を超えない範囲で賠償額を定めることができる懲罰的賠償制度を導入した（営業秘密保護法第14条の2第6項）。

営業秘密侵害行為による損害賠償責任に関する営業秘密保護法第11条では、「故意又は過失」による営業秘密侵害行為に対して損害賠償責任を課しているが、第14条の2第6項の懲罰的賠償規定は、営業秘密侵害行為が「故意」による場合にのみ認められる。したがって、上記の規定の適用を受けるためには、侵害者の「故意」を立証することが重要である。

また、営業秘密保護法第14条の2第7項の各号では、賠償額を判断する際には、①侵害行為をした者の優越的地位の有無、②故意又は損害発生の恐れを認識した程度、③侵害行為によって営業秘密保有者が受けた被害規模、④侵害行為によって侵害した者が得た経済的利益、⑤侵害行為の期間・回数等、⑥侵害行為に伴う罰金、⑦侵害行為を行った者の財産状態、⑧侵害行為を行った者の被害救済努力の程度を考慮することとしている。

したがって、例えば下請関係にある中小企業の営業秘密を大企業が侵害した場合、営業秘密侵害に対する警告状を発送した後継続して侵害行為がある場合、関連刑事事件で罰金刑となった場合などにおいては、賠償額算定時に侵害者に不利に働くことがある。

1.3 証拠収集に係る措置及び手段

(1) 営業秘密保護法第14条の3に基づく資料提出命令

営業秘密侵害を原因とする損害賠償請求の場合、その損害額算定の根拠となる資料が請求人ではなく被請求人の手元にある場合がほとんどである。したがって、営業秘密保護法第14条の3では、営業秘密侵害行為による営業上の利益の侵害に関する訴訟において、当事者の申請により法院が相手方当事者に対し、当該侵害行為による損害額を算定するのに必要な資料を提出することを命ずることができるようにしている。

(2) 提出を拒否する正当な理由

資料提出命令が行なわれた場合でも、その資料の所持者が当該資料の提出を拒絶する「正当な理由」がある場合には、資料提出命令に応じないこともできる。例えば、当該資料を提出することによって、当該資料の保有企業の営業秘密が漏れいし、顕著に甚大な損失の発生が予想される場合などが、上記規定における正当な提出拒否の理由のうちのひとつと見なすことができる。実務的には「正当な理由」が幅広く認められる傾向が強く、制度

の趣旨が失われているという批判がある。

(3) 手続き

当事者は資料提出命令を求める申請書を当該法院に提出する。関連資料が文書である場合には、申請書では民事訴訟法第317条により、文書の表示、文書の趣旨、文書の所持者、証明する事実、文書提出義務の原因を記載しなければならない。

一方、大法院の判例²⁶によれば、文書提出命令を発するにおいて、その文書の存在及び所持者に対する立証責任は文書提出命令を申請する申請人にあるとしているので、営業秘密保護法第14条の3の規定による資料提出義務の場合にも、同一に適用されると判断するのが望ましい。²⁷

1.4 訴訟中の秘密保持に係る措置

2011年10月1日施行の改正営業秘密保護法では、訴訟過程における営業秘密の外部流出を防止するため、日本の不正競争防止法上の秘密保持命令制度に倣い、第14条の4ないし14条の6において秘密保持命令制度を新設した。

(1) 秘密保持命令(営業秘密保護法第14条の4)

営業秘密保護法第14条の4では、営業秘密侵害行為に関する訴訟において、訴訟当事者又は当事者の代理人などが訴訟過程で知り得た営業秘密を、訴訟遂行以外の目的で使用・公開しないよう当該当事者又は代理人などに法院が命ずることができる。

秘密保持命令は、営業秘密保護法第14条の4第1項各号に規定された事由が疎明された場合に限って下されることができる。

(2) 秘密保持命令の取消(営業秘密保護法第14条の5)

営業秘密保持命令を受けた者は、営業秘密保持命令が営業秘密保護法第14条第1項各号の所定の要件を満たさない場合、該当秘密保持命令を下した法院に秘密保持命令の取消しを申立てることができる。

(3) 秘密保持命令が下された資料に対する閲覧制限(営業秘密保護法第14条の4本文)

²⁶ 大法院2005. 7. 11. 宣告2005マ259判決

²⁷ キム・グクヒョン、営業秘密保護法実務、2010年4月1日初版発行、p186

民事訴訟法第163条第1項²⁸所定の秘密保護のための閲覧制限の決定がある場合には、当該決定が下された訴訟記録の閲覧は、当事者に制限される。

しかし、秘密保持命令が下された訴訟に関する訴訟記録の場合、当事者であっても、秘密保持命令を受けていない者が該当記録の閲覧を請求した場合には、その閲覧を一定期間の間制限する。ただし、民事訴訟法第163条第1項所定の秘密保護のための閲覧制限の申立てをした当事者全てが同意した場合には、この限りでない。

(4) 秘密保持命令違反時の罰則(営業秘密保護法第18条の4)

秘密保持命令を受けた者が、正当な理由なしに秘密保持命令に違反して訴訟過程で知り得た営業秘密を訴訟以外の目的で使用・公開した場合には、5年以下の懲役又は5千万ウォン以下の罰金に処する。このような秘密保持命令違反罪は、秘密保持命令を申請した者が告訴しなければならない親告罪である。

1.5 国外での営業秘密侵害行為への処罰

海外への営業秘密流出行為については、営業秘密保護法、産業技術保護法及び防衛産業技術保護法で処罰規定を設けている。これらの法律が適用されるためには、当該法において定められている営業秘密、産業技術及び防衛産業技術の定義を満たさなければならない。一方、産業技術保護法及び防衛産業技術保護法は営業秘密保護法に対する特別法としての性格を有するため、重複適用時は営業秘密保護法に優先して適用されることになる。

[表8]

	営業秘密保護法	産業技術保護法	防衛産業技術保護法
保護対象	営業秘密	産業技術及び国家コア技術	防衛産業技術 (防衛事業庁長の指定及

²⁸ 第163条(秘密保護のための閲覧などの制限) ①次の各号の中でいずれか一つに該当する疎明がある場合、法院は当事者の申立てにより、決定をもって、訴訟記録中の秘密が記述されている部分の閲覧・コピー、裁判・調査中の秘密が記述されている部分の正本・謄本・抄本の交付(以下「秘密記載の部分の閲覧など」という。)を申請できる者を当事者に限定することができる。

1. 訴訟記録中に当事者の私生活に関する重大な秘密が記述されていて、第三者に秘密記載部分の閲覧などを許容した場合、当事者の社会生活に著しい支障を生ずる恐れがあるとき
2. 訴訟記録中に当事者が有する営業秘密(不正競争防止及び営業秘密保護に関する法律第2条第2号に規定された営業秘密をいう。)が記述されているとき
 - ② 第1項の申請がある場合、その申請に関する裁判が確定するまで第三者は秘密記載部分の閲覧などを申請することはできない。
 - ③ 訴訟記録を保管している法院は、利害関係を疎明した第三者の申請により、第1項各号の事由が存在しない、又は消滅したことを理由に第1項の決定を取消することができる。
 - ④ 第1項の申請を棄却した決定又は第3項の申請に関する決定に対しては、即時抗告することができる。
 - ⑤ 第3項の取消し決定は、確定してはじめて効力が生ずる。

		(中央行政機関の長の 指定及び告示)	び告示)
刑事処罰 (既遂犯)	15年以下の懲役又は 15億ウォン以下の罰金 ²⁹	15年以下の懲役、15 億ウォン以下の罰金	20年以下の懲役、20億 ウォン以下の罰金
刑事処罰 (未遂犯)	3年以下の懲役又は3千万 ウォン以下の罰金	3年以下の懲役又は3 千万ウォン以下の罰 金	5年以下の懲役又は5千 万ウォン以下の罰金
民事処罰	侵害禁止、損害賠償及び 信用回復請求権	侵害禁止請求権	-

1.6 営業秘密侵害物品に対する水際措置

(1) 営業秘密侵害品の没収

営業秘密保護法では、営業秘密侵害品に関する没収規定を別途設けていない。ただし、産業技術保護法(第36条第5項)及び防衛産業技術保護法(第21条第5項)では、侵害行為によって得た財産を没収できるようにしている。

(2) 輸出入通関保留措置の可否

関税法第235条によると、知的財産権を侵害する物品の場合、輸出又は輸入を禁止しており、この条項に基づいて権利者の要請がある場合、侵害品の輸出入通関を保留させることができる。

ただし、輸出入通関に適用される知的財産権は商標法、著作権法、食品新品種保護法、農水産物品質管理法、特許法、デザイン保護法に登録されている権利である(関税法第235条)。したがって、営業秘密保護法によって保護される権利は含まれないため、営業秘密を侵害した物品については上記の措置がとれない。

(3) 不公正貿易防止法に基づく輸出入禁止措置

(a) 不公正貿易行為の調査及び産業被害の救済に関する法律(以下「不公正貿易防止法」という。)第4条第1項第1号では、特許権、実用新案権、デザイン権、商標権、著作権、営業秘密等(以下「知的財産権」という。)を侵害する物品を国内に輸入あるいは輸入した知的財産権侵害物品を国内で販売する行為、又は知的財産権侵害物品を輸出あるいは輸出の目的で国内で製造する行為は不公正貿易行為とみなし、禁止している。

したがって、営業秘密保有者は、営業秘密侵害が発生した場合、その違反内容の証拠資料を添付して貿易委員会に不公正貿易行為調査を申請することができる。

貿易委員会はダンピングや知的財産権侵害のような不公正貿易行為などによって国内産

²⁹ 違反行為による財産上の利得額の10倍に相当する金額が15億ウォンを超えると、その財産上の利得額の2倍以上10倍以下の罰金に処する。

業が被害を被る、あるいは公正な貿易秩序を害する恐れがある場合、これを調査・判定するために1987年に設立された機関で、韓国産業通商資源部所属の行政機関である。

(b) さらに、不公正貿易防止法第14条の2に基づく「既判定物品確認制度」によると、第三者の物品が営業秘密を侵害したものと既に判定された物品と同一のものと貿易委員会が判定した場合、正当な権原なしになされた第三者の行為は不公正貿易行為とみなされる。このような既判定物品確認制度によると、物品の同一性及び行為者の正当な権限の有無のみを判断して、不公正貿易行為であるか否かを判定するため、簡便かつ迅速に進められるというメリットがある。

(c) 貿易委員会により不公正貿易行為と判定される場合、貿易委員会は侵害者に対し、侵害行為の中止、侵害物品の搬入排除及び廃棄処分等の是正措置を命じる。また是正措置に応じない場合、3年以下の懲役又は3千万ウォン以下の罰金に処される。

2. 最近の判例の動向³⁰

下記判決の統計は、2017年1月1日から2019年12月31日までの全国各級の法院の営業秘密保護法に関する民事仮処分、民事本案、刑事判決文1960件を分析対象として法務法人ダウムが分析し、作成した「不正競争防止及び営業秘密保護に関する法律判決文の分析研究」最終報告書における分析データによるものである。

2.1 営業秘密侵害行為の類型(民事本案)

民事本案事件において、営業秘密侵害の類型及びそれに対する法院の判断結果をみると、侵害行為の類型を明示しないケースが70%を超え、この場合、認容率は侵害行為の類型を特定したケースと比べて著しく低かった。

また、請求が棄却された場合の棄却事由をみると、秘密管理性が否定された割合(30.1%)が最も高く、次に非公知性が否定された割合(23.5%)が高かった。

[表9]

行為 類型	認容の有無			棄却事由					
	認容	判断なし	棄却	営業秘密の特定	非公知性	経済的有用性	秘密管理性	転職・競争禁止約定の無効	その他
第三者不正取得 (イ～ハ目)	11	－	17	2	9	4	7	1	6
秘密保持義務者の不正公開 (ニ～ヘ目)	14	－	17	2	8	6	6	2	7
不明	27	2	138	17	51	41	74	15	31
合計	52	2	172	21	68	51	87	18	44

³⁰ 不正競争防止及び営業秘密保護に関する法律判決文の分析研究、特許庁、2020

2.2 民事事件の認容率(本案)

民事本案事件における処理結果をみると、第1審で侵害禁止、損害賠償請求などが認容された割合は38.9%となっており、信用回復が請求された事件はなかった。また、上告審で下級審の判決が覆されたケースはないことがわかる。

[表10]

請求内容	第1審		控訴審		上告審	
	認容	棄却	控訴認容	控訴棄却	破棄差戻し	上告棄却
侵害禁止	16	33	11	7	－	8
損害補償	110	173	37	34	－	5
信用回復	－	－	－	－	－	－
その他	1	2	1	－	－	1
合計	127	208	49	41	－	14

2.3 刑事事件の認容率

刑事本案事件における処理結果をみると、第1審で有罪が宣告された割合は38.5%で、民事本案で請求が認容された割合とほぼ類似していることがわかる。また、民事本案と同様、上告審で下級審の判決が覆されたことはないことがわかる。

したがって刑事訴訟で勝訴するためには、事実審の第1審、第2審で有利な判決が得られるよう注力する必要があると思われる。

[表11]

第1審			控訴審		上告審	
有罪	無罪	その他	破棄	控訴棄却	破棄差戻し	上告棄却
74 (60.7%)	47 (38.5%)	1 (0.8%)	11 (61.1%)	7 (38.9%)	－	8 (100%)

2.4 損害賠償額の算定

民事本案で営業秘密侵害による損害を認め損害額を算定した事件において、賠償額の分布を見ると以下のとおりである。

下表からわかるように、法院が弁論全体の趣旨等に基づいて損害額を算定した場合が76.9%に達しており、営業秘密保護法上の損害額推定規定の存在があるにもかかわらず、損害額立証の困難が解消されていないことがわかる。

また、認められた賠償額及び請求額に対する認められた賠償額の割合の側面においては、法院が認めた相当損害額の場合が最も低いことがわかり、損害額を十分認めてもらうには損害額を積極的に立証する必要があると考えられる。

[表12]

算定の根拠	賠償額の分布	平均

	1千万 ウォン 以下	3千万 ウォン 以下	5千万 ウォン 以下	1億ウ ォン以 下	3億ウ ォン以 下	5億ウ ォン以 下	5億ウ ォン超 過	賠償額 (対請求額比 認容率)
侵害物件 譲渡利益額	-	-	-	-	1	-	1	4,357,472,885 (51.33%)
侵害者の 利益額	2	-	-	-	-	-	1	306,770,287 (56.46%)
通常実施料 相当額	-	-	-	1	-	-	-	75,866,024 (65.50%)
法院認定 相当損害額	1	6	4	2	2	1	4	298,446,424 (36.69%)
不明	-	-	-	-	-	-	-	-
合計	3	6	4	3	3	1	6	603,078,890 (41.21%)

一方、2019年改正の営業秘密保護法では、3倍上限制方式の懲罰的損害賠償制度を導入した。ただし、現在まで公開された判決文では、懲罰的損害賠償制度により損害賠償額が算定されたケースは見つからなかった。

2.5 刑事訴訟における量刑分布

刑事訴訟における量刑分布をみると、国外での営業秘密侵害の場合、自由刑と財産刑ともに国内侵害に比べて量刑基準はるかに高いにもかかわらず、実際の量刑は国内侵害よりも低いことがわかる。

また、自由刑と財産刑のいずれも法廷最高刑と比べかなり軽い刑が宣告されていることがわかる。

[表13]

侵害類型	自由刑					財産刑					
	8月以下	1年 4月以下	2年以下	3年以下	3年超 過	1百万 ウォン 以下	3百万 ウォン 以下	5百万 ウォン 以下	1千万 ウォン 以下	3千万 ウォン 以下	3千万 ウォン 超過
国外侵害	2	8	-	-	-	-	-	-	4	-	-
国内侵害	25	16	12	-	-	-	8	9	11	6	2
不明	2	4	-	-	-	-	-	4	-	1	-

2.6 秘密管理性の要件緩和に関する判例の態度

営業秘密保護法では、2015年及び2019年の2回の改正を通じて、秘密管理性の要件を徐々に緩和している。これに関して、営業秘密民事本案における秘密管理性の認容率をみると、以下のとおりである。

以下の結果をみると、2回の改正を通じて秘密管理性の要件が緩和されているにもかかわらず、実際の判決時に秘密管理性が認容される割合がさらに低くなっており、未だ改正の趣旨が判決の結果につながっていないことがわかる。

[表14]

秘密管理性の規定		合計	秘密管理性の認容率	
適用法律	定義		認定	否定
2015年以前旧法	相当の努力	90	23 (25.5%)	67
2015年改正法	合理的努力	58	11 (18.9%)	47
2019年改正法	合理的努力	3	－ (0%)	3
合計		151	34 (22.5%)	117

第 2 編 営業秘密漏洩対策実践編

営業秘密として保護される知識資産は、該当企業が長い時間と費用をかけて形成したものであって、企業収益創出の源泉であり、流出時にはその回収や回復が困難であって、企業に回復できない被害を発生させることとなる。したがって、営業秘密が流出しないよう事前に防止することが最善の措置であり、営業秘密が流出した場合、被害がさらに大きくならないよう速やかに対応することが重要である。

以下本編では、営業秘密の流出を防ぐための管理体系の構築方法、及び民事・刑事上の措置を含む流出時の対応方法について説明する。

第 1 章 総論(営業秘密の管理方法)

1. 自主的な営業秘密管理体制の構築

1.1 合理的な営業秘密保護管理体制構築の必要性

営業秘密として管理される情報は、当該企業の長年の努力と投資の成果物であり、企業の競争力の中核をなすもので、一旦侵害が発生すると、当該情報の回収や回復は極めて困難である。したがって、極度に激化する国際競争社会において、企業が生存するためには営業秘密の徹底した保護管理が重要となる。

したがって、営業秘密の保護管理において、経営者は営業秘密のこうした特性を考慮して戦略的で経営的な資源を投資する必要がある。

また、他の面においては、一定水準以上の営業秘密の保護管理体系の存否は、営業秘密の侵害時に法的保護を受けるための重要な一要件(秘密管理性)となっている。

ただし、企業が保有する知識資産をすべて営業秘密として管理することは管理コストが過度に高くなり、管理効率と業務効率を低下させてしまうこととなる。

したがって、企業は自社の経営や事業戦略に合わせて営業秘密として管理すべき情報を厳選した上で、流出リスク、管理コスト、業務効率等を考慮して合理的な管理を行う必要がある。

1.2 営業秘密を効果的に保護できる管理体系の構築

(1) 社内における営業秘密の管理及び共有方法

営業秘密が記載、記録されている媒体には、営業秘密である旨を表示して他の媒体と分離して保管し、当該媒体を外部へ持ち出すことと複製することについては原則として禁止することが望ましい。

また、営業秘密にアクセスできる職員を制限し、他部署の者は閲覧できないようパスワードを設定し、当該パスワードの有効期間を設定するとともに、同一又は類似パスワードの使用を制限する措置が必要である。

また、DRM(Digital Rights Management)システム、統合認証権限管理(Extranet Access Management)システム、知識管理システム(Knowledge Management System)等を情報管理システムとして採用し、特定の情報に対してアクセス可能な人員を指定管理し、当該情報にアクセス、出力及び流出した記録を追跡可能にすることが望ましい。

(2) 社外への営業秘密の管理及び共有方法

韓国の企業文化の特性上、大企業と中小企業間の関係は共生関係というよりは垂直的な上下関係に近い。したがって、大企業と中小企業間の下請取引の際には、大企業が取引上

優越した地位を利用して不当に技術情報の提供を求めることが多い。

したがって、取引対象である大企業から口頭で技術資料提供を求められたときは、技術資料の名称及び範囲、要求目的、要求日、引渡し日、引渡し方法、秘密保持に関する事項、権利帰属関係、技術資料の対価等を記載し書面化された技術資料要求書の交付を要求する必要がある。

また、技術資料提供合意の際は、技術資料の使用態様及び範囲の使用対価の有無及び金額、提供された技術資料の秘密保持義務等について書面化された合意書を作成する必要がある。一方、2021年8月17日に公布された改正下請法（2022年2月18日施行予定）においては、下請事業者が親事業者に対し技術資料を提供する場合、親事業者が下請事業者と技術資料について秘密保持契約を締結するよう義務づけている。

もし大企業が書面化された技術資料要求書を交付しない、あるいは技術資料要求書で規定した技術資料の範囲外の技術資料を要請する場合、正当な事由のない技術資料の提供に該当し、下請法第12条の3第1項に規定された、正当な事由のない技術資料の提供に該当することを抗弁することができる。

また、大企業が書面化された合意書に規定された秘密保持義務に違反して技術を利用、あるいは第三者に利用させた場合、又は技術提供の目的から外れて技術資料を活用する場合などは、下請法第12条の3で規定している技術資料流用行為に該当することを抗弁することができる。

（3）韓国内支社と本社間の営業秘密共有方法

韓国内支社と日本本社間の営業秘密共有の際は、外部流出が相対的に容易な電子メールを利用するより、前述のようにDRMシステム、統合認証権限管理システム（EAM）や知識管理システム（KMS）を利用して共有することが望ましい。

韓国内支社と日本本社間において海外出張などを通じて営業秘密を共有する場合、次のような措置³¹を取る必要がある。

〔表15〕

段階	状況	規則
出国前	事前準備	不要なハードウェアや情報は持たず、すべての情報はバックアップしておき、ハードウェアには8文字以上のパスワードを設定。 ハードウェアに入っている情報は全て暗号化し、ファイアウォールプログラムを設定。
	手荷物発送	ハードウェアは常に携帯し、本体やケースにパスワード、電話番号などを記録しない。 無認可の個人用ノートパソコンの使用及び携帯を禁止する。 ハードウェアにセキュリティシールを貼り付ける。
出張中	ホテル利用	ハードウェア、USBは常に携帯し、ホテルの客室など

³¹ 中小企業のためのR&Dセキュリティマニュアル、中小企業技術情報振興院の情報システム支援室

		に放置しない。
	公共施設利用	業務上のセンシティブな情報については言及せず、意図が不明な質問等には無視するか、あるいは明確でない回答に一貫する必要がある。
	秘密転送及び口外	秘密やセンシティブな情報を転送する際は現地のパソコン、ファックスや電話を使用しない。
帰国後	秘密転送及び口外	帰国後早期にハードウェアのパスワードを変更。出張中に使用したハードウェアについては悪性プログラムがインストールされていないか確認。

1.3 法的保護を受けることができる営業秘密保護管理体系の構築

営業秘密保護法による法的保護を受けるためには、営業秘密保護法上の営業秘密の成立要件を満たす必要がある。特に営業秘密として認められるためには、秘密管理性の認定の有無が重要である。韓国では、累次の改正を通じて秘密管理性の認定要件を緩和し続けているが、現在まで大法院で行われた判決を見てみると、秘密管理性が否定され、訴訟が棄却される事例が少なくない。

秘密管理性の認定要件に関して、韓国大法院の判例は「その情報が秘密と認識され得る表示をするか、告知をし、その情報にアクセスできる対象者やアクセス方法を制限するか、その情報にアクセスした者に秘密遵守義務を課すなど、客観的にその情報が秘密に保持管理されているという事実が認識可能な状態であること」³²と判示している。

上記の判決は、2015年改正以前の旧法上、「相当な努力により秘密として保持」されることの意味を説いたものであるが、改正以降の判例の傾向からみて、上記の判断基準に大きな変化はないものと考えられる。

したがって、営業秘密保護法の保護を受けることができる営業秘密として認められるためには、営業秘密保有者の単なる主観的意思だけでは足りず、客観的にその秘密管理の有無が表出されることが重要である。

そのためには、営業秘密保護体系を構築するにあたって、以下の3点が遵守される必要がある。

(1) 営業秘密の指定及び表示

当該情報にアクセスする者に対して、それが営業秘密であることを認識できるよう文書に表示を付す等の措置

(2) アクセス権者の制限及び営業秘密保護義務の賦課

当該情報にアクセスできる者を制限したり、既にアクセスした者から取得した情報を個人的に使用・公開することに一定の制限を加える（秘密保護協定等を締結）

³² 大法院2008. 7. 10. 判決2008ド3435判決

(3) 物理的制限

当該情報を一定の場所等に保管し、そのアクセスが認められる者以外は物理的にアクセスを制限(保管場所に施錠、パスワード等を設定)

2. 営業秘密保護センターの営業秘密管理システムの導入

資金力や技術力に欠ける中小企業が、上記の営業秘密管理体系を構築することは容易ではない。したがって、韓国特許情報院では、このような中小企業の困難性に対して援助をするため、営業秘密登録・等級付与、取扱人員・権限及び履歴管理、セキュリティ誓約書管理、原本証明などの営業秘密管理機能を実現して開発した営業秘密管理システムを提供している。

2.1 システムの構成及び利用方法

(1) システムの構成

営業秘密管理システムは以下のような機能を提供する。

[表16]

秘密文書管理	アクセス権管理	人材管理	履歴・統計管理	マイページ
営業秘密資料の登録・修正・搬出、営業秘密原本証明サービスの連携	利用者別権限設定及び利用グループの構成、総管理者の指定	組織内の利用者登録、管理者有無の指定、誓約書の徴求及び管理	利用者別営業秘密資料取扱履歴照会、登録・閲覧・修正・搬出に関する統計確認	自身がアクセス可能な営業秘密資料の確認、同一アクセス権を持つ利用者の確認

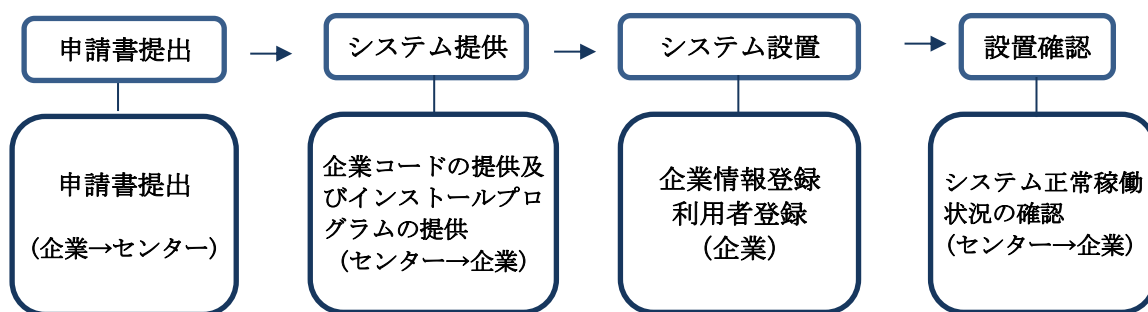
(2) サービス申請

営業秘密標準管理システムの利用を希望する者は、営業秘密保護センターホームページの営業秘密管理システム申込ページ³³から申請できる。

(3) サービスの利用手続き

営業秘密管理システムは以下のような手続きに従って利用できる。

³³ <https://www.tradesecret.or.kr/info/systemIntro.do?gb=331>



(4) システムの使用方法

企業内総括管理者のパソコン及び利用者のパソコン内に営業秘密保護センターが提供するエージェントプログラムを設置することにより、営業秘密資料の登録及び管理が可能となる。この場合、総括管理者のパソコンとつながっているウェブサーバーに営業秘密を保存することとなる。

また、余備のパソコンを保有する場合は、当該パソコンに営業秘密保護センターから提供するウェブサーバープログラムを設置し、当該ウェブサーバープログラムに接続されたウェブサーバーに営業秘密を保存する。

2.2 長所

(1) 営業秘密の保護及び管理コストの削減

営業秘密保護システム構築のためのサーバ・商用ソフトウェアの導入又は独自ソフトウェア開発等のシステム構築費用は不要であり、営業秘密保護センターから提供する原本証明サービスを併せて利用する場合、実質的に無償で利用できる。

(2) 秘密管理性の立証が容易

営業秘密管理システムを通じて、秘密取扱記録、秘密アクセス権、従業員誓約書、最近の動向記録等の営業秘密管理履歴を生成・保管することにより、今後営業秘密流出に係る訴訟において、当該技術が秘密として保持された情報であることの立証が容易となる。

また、営業秘密利用についての権限設定により、保有者及び取扱者のみが秘密情報の取扱いが可能であるという部分立証が可能であるため、当該技術の非公知性を立証しやすくなる。

(3) 利用者の認識を改善

営業秘密管理システムの活用を通じて、秘密流出に対する職員の警戒心を高め、営業秘密に対する認識転換のきっかけを作ることができる。

2.3 利用費用

営業秘密管理システムの場合、営業秘密保護センターの支援事業の利用実績³⁴があれば無償で提供され、利用実績のない企業は加入費10万ウォンで利用できる。

ここでの加入費10万ウォンは営業秘密保護センターから提供する原本証明サービスの利用が可能な10万ポイントとして払い戻される。したがって、原本証明サービスの利用の際は、実質的に無償で営業秘密標準管理システムの利用が可能になる。

3. 営業秘密の登録

3.1 技術資料任置制度の活用

技術資料任置制度は、中小企業が開発したソースコード及び生産方法など技術関連資料を政府が指定した信頼性のある第三者機関（大・中小企業・農漁業協力財団）に任置した後、契約手続きによって委託企業に任置された技術資料を交付・管理することである。

（1）所管機関及び法的根拠

技術資料任置制度は、大・中小企業の共生協力の促進に係る法律第24条の2に基づくもので、大・中小企業・農漁業協力財団の技術任置センターが技術資料の保管及び交付を担当する。

技術資料の任置は、契約当事者間の合意により進めることができ、契約書によらない限り当該制度を利用する義務はない。

（2）任置契約の類型

（a）多者間任置契約

中小企業が多数の大企業に技術を納品・供給する場合、まず中小企業と大・中小企業・農漁業協力財団が任置契約を締結した後、多数の大企業が契約に編入できる契約類型である。

（b）三者間任置契約

特定企業との特許ライセンス契約のように、中小企業が単一の大企業に技術を納品・供給する場合、中小企業と大企業及び大・中小企業・農漁業協力財団の三者が合意して任置契約を締結する契約類型である。

³⁴営業秘密保護コンサルティング、企業訪問教育、初動対応法律諮問、原本証明サービス、統合管理支援プログラム

(3) 技術資料任置の対象

(a) 技術上の情報

施設及び製品の設計図/物品の生産及び製造方法、物質の配合方法/研究開発報告書及びデータ、ソフトウェアソースコード及びデジタルコンテンツなど

(b) 経営上の情報

企業の運営及び管理に関する機密書類(財務、会計、人事、マーケティング、労務、生産)、企業の売上に関する機密書類(原価、取引先、各種報告書及びマニュアル)

(c) 産業財産権に関する情報

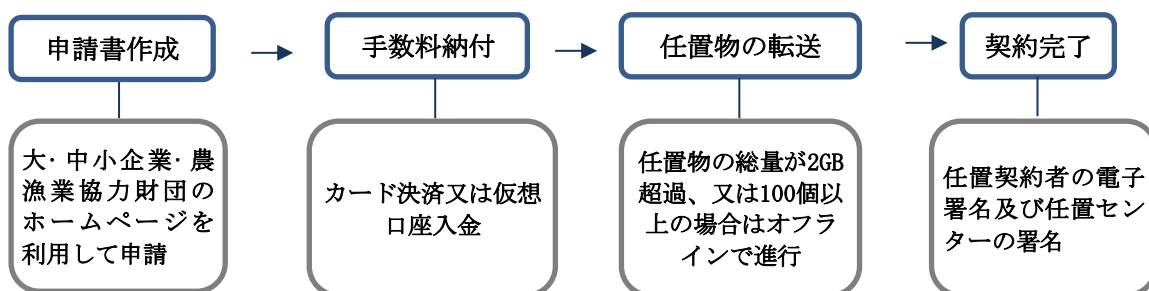
特許権、実用新案権、デザイン権などの産業財産に関する情報

(4) 利用方法

(a) 企業会員加入及び汎用共同認証書の登録

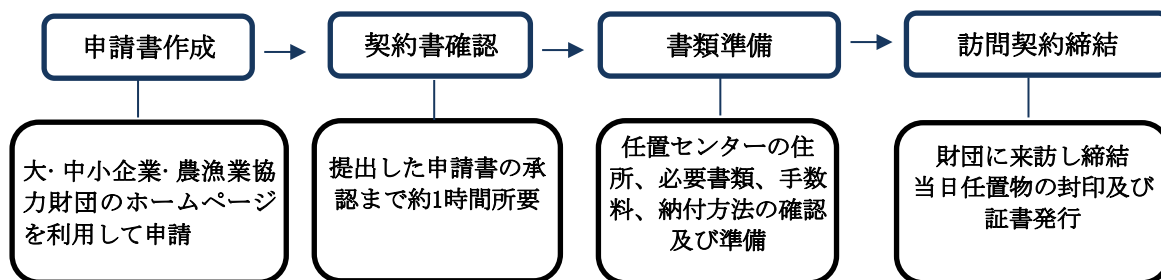
大・中小企業・農漁業協力財団の会員登録ホームページ³⁵で会員登録後、使用が可能である。加入の際には汎用共同認証書が必要で、汎用共同認証書の発行及び使用が困難な場合は、技術資料任置センター事務室に来訪し、オフラインでの契約締結も可能である。

(b) オンライン利用(大・中小企業・農漁業協力財団のホームページを利用)



(c) オフライン利用(大・中小企業・農漁業協力財団を訪問し、契約締結後に任置)

³⁵ <https://kescrow.or.kr/tems/mem/terms2.do>



(4) 技術資料の交付手順

技術資料が任置された後、技術資料の交付条件が発生した場合、委託企業の技術資料の交付要求によって、任置機関である受置人は技術資料を委託企業に交付する。

共生法第24条の2第2項において、任置物の交付要請の条件を挙げているが、委託企業は、次の4つの条件のうちいずれか一つが発生した場合、任置機関に任置物の交付を要請することができる。第一に、受託企業が同意した場合、第二に、受託企業が破産宣告を受けたり解散決議をしてその権利が‘民法’又は他の法律によって消滅した場合、第三に、受託企業が事業場を閉鎖して事業が不可能な場合、第四に、委託企業と受託企業が協議して定めた交付条件に合致する場合などを明示している。

(5) 任置手数料

[表17]

契約類型	手数料(件/年)	備考	
新規	(一般) 300,000ウォン/年 (減免 ³⁶) 200,000ウォン/年	類型別新規技術資料任置契約	ただし、5年以上任置契約を締結する場合、手数料の1/2減免
更新	(一般) 150,000ウォン/年 (減免) 100,000ウォン/年	維持中の任置契約の更新	
編入	50,000ウォン	既存の両者間契約に使用者が編入する場合	
追加	50,000ウォン	技術資料の追加事由が発生し、任置物として追加	

(a) 技術資料の安全な利用保障

技術任置サービスを利用すれば、技術開発企業が破産や廃業又は自然災害により技術を滅失した場合でも、使用企業が任置機関により任置された技術の交付を受け、メンテナン

³⁶ 青年創業企業バウチャー事業の対象

スを行うことができる。

(b) 技術奪い取りの防止

任置された技術資料は所定の交付条件発生に限り委託企業に提供される。従って、中小企業が大企業との取引の際、技術任置サービスを利用すれば、委託企業である大企業が取引上優越的な地位を利用し、受託企業である中小企業を相手に任置された技術情報を奪い取る行為から技術開発企業を保護することができる。

(c) 知的財産権の保護及び費用削減

技術開発企業の立場において、技術任置サービスを利用すれば、知的財産権を使用企業に譲渡することなく、基盤技術として保有したまま、既存技術の修正補完により新たな技術開発ができ、費用削減の効果が期待される。

技術を使用する企業においても、技術開発企業から知的財産権の一切を引き受けることに比べ、低コストで技術を利用することができ、費用削減の効果が期待される。

(d) その他

日本企業が自社の製品を韓国に輸出する際、韓国企業が日本企業からの技術提供が中断される可能性を懸念して契約締結を敬遠する場合、技術任置契約を通じて問題を解決することができる。

また、任置時点を通じて技術保有時点を間接的に類推できるため、技術開発及び保有時点が争点となる営業秘密関連の訴訟や先使用权の立証が必要な訴訟などにおいて、有力な立証資料として活用可能である。

(6) 技術資料任置制度の限界

取引上優位な立場にある委託企業が任置機関と両者契約を通じて技術資料を任置した場合でも、自らの優越的な地位を利用して受託企業に任置物の交付を直・間接的に強要する場合、取引を継続しなければならない受託企業としては、委託企業の要求に同意せざるを得ない、現実的な問題点が依然として存在する。

なお、大・中小企業共生協力促進に関する法律第28条第1項第4号³⁷によると、技術資料の任置について委託企業と受託企業間とで紛争が発生した場合には、中小企業庁長に紛争調停を要請することができる。

37 第28条(紛争の調停) ① 次の各号の事項について委託企業と受託企業又は中小企業協同組合間に紛争が生じたときには、委託企業・受託企業又は中小企業共同組合は大統領令で定めるところにより、中小企業庁長に紛争調停を要請することができる。

1. 第21条による約定書及び物品受領証に関する事項
2. 第22条による納品代金の支払などに関する事項
3. 第23条による物品などの検査に関する事項
4. 第24条の2による技術資料の任置に関する事項

3.2 営業秘密原本証明制度の活用

営業秘密原本証明制度は、企業が保有している技術資料の原本性を立証する制度である。企業が保有しているコア技術は、自社が保管し、当該ファイルの生成時点などを立証できる暗号化されたファイルのみを第三者機関に保管しておくことにより、企業が保有している電子文書の生成時点及び原本の存在の有無について第三者機関が証明する制度である。

(1) サービスの概要

営業秘密原本証明サービスは、営業秘密が盛り込まれた電子文書は企業や個人が保管しながら、タイムスタンプ(time stamp)³⁸という電子的技術を用いて、電子文書から抽出された電子指紋(hash code)³⁹をタイムスタンプ発給機関が保管し、必要時にはタイムスタンプ発給機関が保存している電子指紋と電子文書に発給されたタイムスタンプとを比較することにより、その生成時点と原本であるか否かを確認する方式である。

(2) 所管機関及び法的根拠

このサービスは、韓国特許庁傘下の「韓国特許情報院(www.tradecret.or.kr)」の営業秘密保護センターにおいて運営されており、原本証明機関の法的根拠は、営業秘密保護法第9条の3である。

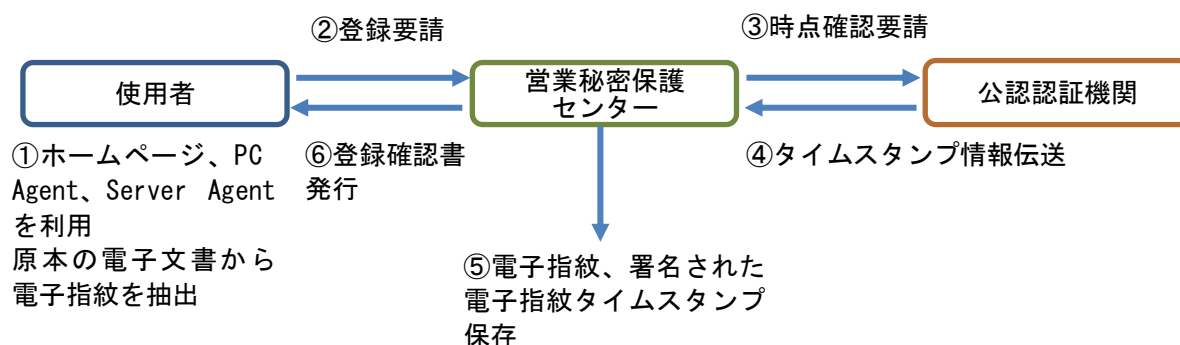
(3) サービスの種類

(a) 原本登録サービス

使用者がシステムに電子文書を登録要請すると、電子文書から抽出した電子指紋と公認認証機関の時間情報によって当該営業秘密の存在と保有時点を営業秘密保護センターに登録するサービスである。

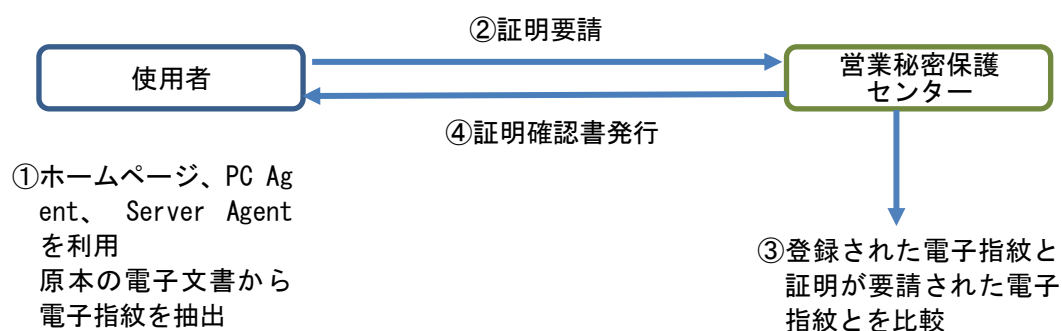
³⁸ ある時点にデータが存在していた事実を証明するために、特定の位置に表示する時刻で、共通に参考とする時刻について時間の起点を表示する時間変化パラメータ。

³⁹ 電子文書から乱数を生成する手法によって生成される値で、電子文書が修正されれば他のコードが生成され、ハッシュコードを元の電子文書に戻すことはできない。



(b) 原本検証サービス

使用者が保有している電子文書の原本証明を要請した場合、当該電子文書から電子指紋を抽出し、営業秘密保護センターで保管中の電子指紋と比較して原本であるか否かを検証するサービスである。



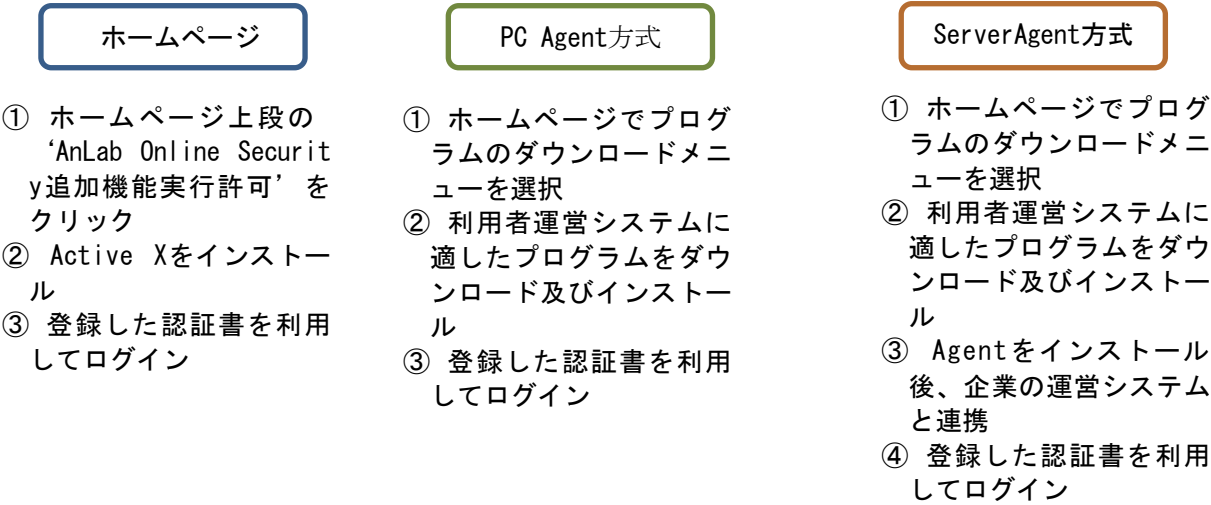
(4) サービスの利用方法及び手順

(a) サービス登録方法

営業秘密原本証明サービスを利用するためには、まず韓国特許情報院のホームページ(www.tradesecret.or.kr)を通じて会員登録し、会員登録後、ホームページ内の[認証書の登録]を選択して加入時に付与されたパスワードと事業者登録番号又は住民登録番号を入力し、保有している汎用又は金融専用認証書を登録する。

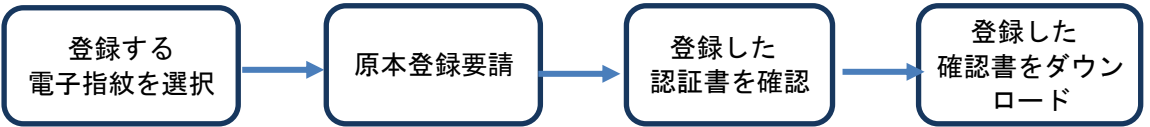
(b) サービスへのアクセス及び利用方法

使用者は、営業秘密原本証明サービスのホームページに直接アクセスして利用する方法、別途システムがない中・小企業又は個人の利用者の場合は、Agentを直接自身のパソコンにインストールして利用するPC Agent方式、又は企業の既存運営システムと連動して原本登録及び原本検証サービスを直接利用するServer Agent方式のうち、いずれか一つを選択して利用する。

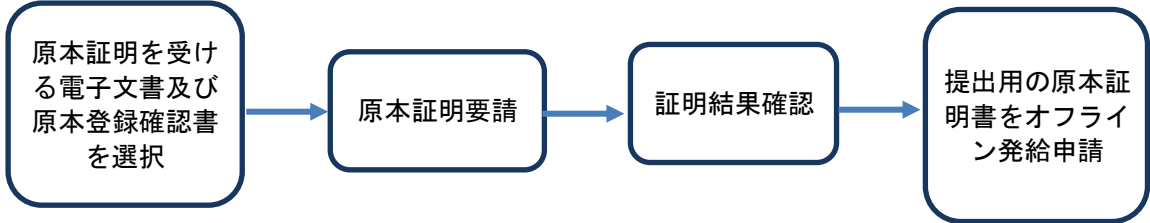


(c) サービスの利用手順

① 原本登録サービス



② 原本証明サービス⁴⁰



(5) 費用

[表18]

区分		単価	備考
原本証明サービス	新規登録	10000ポイント ⁴¹ / (件・1年)	新規原本登録時
	維持登録	3000ポイント/ (件・1年)	維持期間内の更新時
	割増維持登録	9000ポイント/ (件・1年)	維持期間終了後6ヶ月以内の更新時

⁴⁰ 原本証明書は法院提出の用途に使われ、オフラインでのみ発給可能。ただし、原本登録確認書はマイページを通じてオンラインで確認可能。

⁴¹ 事前購入後に利用可能(1ポイント=1ウォン、付加価値税込み)

原本証明書の発給	30000ポイント /(件・1年)	

(6) 長所

(a) 訴訟での立証責任の緩和と証拠資料の確保

原本証明サービスを利用すると、特定時点に特定の営業秘密が存在していたという事実の立証が容易になり、営業秘密保持者の立証責任が緩和される。特に、他社へ転職した職員による競合他社への営業秘密流出行為のように、営業秘密間の生成順序や完成時点に関する事実関係が争点となる事案では重要な証拠資料として活用できる。

(b) 営業秘密流出行為の事前予防

営業秘密に対して原本証明を受けておけば、以後企業内の役職員による営業秘密の流出時に、タイムスタンプを利用した検証手続きを通じて営業秘密侵害の責任を問えるため、営業秘密の流出行為を事前に防ぐ効果がある。

(c) 営業秘密の秘密保持性の立証が容易

営業秘密原本証明サービスを利用する場合は、営業秘密保護法上の保護対象である営業秘密として認められるための秘密保持性を立証しやすくなる。

(d) 先使用権の立証が容易

企業が秘密裏に開発している技術について、他人が特許出願して登録された場合は、登録特許権によって該当技術の実施が制限されることがある。この場合、企業が開発している技術に対し営業秘密原本証明サービスを利用して原本証明を受けておけば、他人の登録特許の出願時点以前に当該技術を保有していたということを容易に証明することができ、先使用権が認められる可能性が高い。

(7) 原本証明サービス制度の限界

(a) 営業秘密立証の問題

営業秘密原本証明サービスは、営業秘密の生成時点に関する証明のみをサービスするための制度であって、登録した電子文書が営業秘密に該当するかどうかを立証するサービスではない。したがって、原本の内容が営業秘密に該当するかは企業自らの判断が必要であり、これを法廷で立証することは依然として困難を伴う可能性がある。

(b) 利用手続き上の問題 ⁴²

⁴² 韓国特許庁、企業の技術流出防止のための営業秘密管理方案及び保護制度の研究、2011. 12.

営業秘密原本証明サービスでは、営業秘密それ自体は該当機関に任せず、企業自らが保管しているため、流出防止のための徹底した管理が必要である。

また、企業内部の人材、システム障害などによって保管していたデータに損傷が加わった場合、原本とはハッシュコード値が変わり、原本時点の立証が困難になるという問題点がある。

現在、営業秘密原本証明サービスでは、電子文書1件当たり一つの電子指紋のみを持つことになる。したがって、企業の持続的な技術開発を通じてその内容が修正・変更される場合には、その度に新しい電子指紋を抽出しなければならず、原本登録のために同一の手続きを繰り返さなければならないという煩わしさがある。

第 2 章 管理体制整備のステップ 1ー管理体制の現状の確認

1. 現状把握の必要性

営業秘密管理体制を導入し、維持するには多くの時間と人員及び費用が必要となる。特に必要となる人員、費用等は、どのような情報まで営業秘密として保護するのか、及びどのレベルまで営業秘密保護体系を構築するのかによって大きく変わることになる。

従って、企業は競合他社に比べて優位を確保できる強みとなる情報を選定するため、まず自社が保有している情報を把握することが重要である。すでに公知の情報や競合他社に比べて技術的優位を確保できない情報まで管理体系内に置くことは、人的・物的浪費であるためである。

また、目標とする営業秘密の管理水準を設定し、現在企業が保有している営業秘密保護管理体系を把握し、整備が必要であったり、新たな体系の導入が必要な部分を適切に判断する必要がある。

例えば、営業秘密保護法による保護を受けられる水準(秘密管理性)の管理体系を目指すのか、そうでなければ、営業秘密の流出を根本的に防止できる程度の高水準の管理体系を目指すのかを決定する必要がある。

また、各営業秘密ごとに下記のようなセルフチェックリストを作成し、各項目ごとに現在の管理レベルを把握することにより、補完が必要な項目を発見することが重要である。

一方、韓国における営業秘密保護法違反事件の無罪率が19.8%⁴³(全刑事事件の無罪率3.4%)と高く、民事訴訟によって認められる損害賠償額が高くなく、一度流出するとその損害の原状回復が事実上不可能な営業秘密の特性を考慮すると、営業秘密保護法上の秘密管理性が認められる水準を超えて、営業秘密の流出を根本的に防止できる高い水準の管理体系を構築することが求められる。

⁴³ 不正競争防止及び営業秘密保護に関する法律判決文の分析研究、特許庁、2020

2. セルフチェックシート

[表19]

カテゴリー	項目
政策管理	☐ 営業秘密の対象に対してアクセス統制基準を持って統制し、権限変更及び調整時にアクセス権限を回収している。
	☐ 毎年1回以上全従業員に対して定期的に営業秘密教育を実施している。
	☐ 営業秘密管理規程が社規に盛り込まれており、その遵守の可否を毎年監査している。
	☐ 社内又は部署別に営業秘密の管理責任者が指定されている。
取扱管理	☐ 会社の重要情報や資料等を管理台帳に営業秘密として登録している。
	☐ 登録された営業秘密文書の表紙や電子文書フォルダなどに秘密である旨が表示されている。
	☐ 営業秘密が記録された媒体を他の文書と区別して保管、あるいはアクセス制限措置された情報システムに保管している。
	☐ 営業秘密の登録、配布、閲覧、印刷、社外への持ち出し、保管など全般的な管理状況を電子情報システムで記録管理している。
	☐ 営業秘密へのアクセス権を持たない者は管理責任者の許諾を得て閲覧・使用し、その事実を閲覧記録表等に記録している。
	☐ 営業秘密の複製・印刷を原則禁止、あるいは制限している。
	☐ USB、PC、金型、試作品等営業秘密の社外持ち出し及び回収に対する許可手続きを備え、それらを遵守している。
	☐ 営業秘密の廃棄方法が規定されており、その方法通りに実行している。
人的管理	☐ 定期的又は年俸交渉時又はプロジェクト参加時、退職時に営業秘密保護誓約書を徴求して保管している。
	☐ 外部者(協力会社、コンサルティング、契約者等の取引者など)に対する営業秘密公開/閲覧が必要な場合は、秘密保持契約締結又は誓約書を徴求している。
	☐ 従業員に対する営業秘密保護義務を社規で規定している。
	☐ 退職後、一定期間まで退職者の動向を管理。
	☐ 営業秘密管理規程違反時の懲戒規定を備えており、実際にこれを適用している。
物理的管理	☐ 重要施設を統制区域に指定し、施錠装置などで出入りを統制している。
	☐ 外注業者、アウトソーシング業者、契約者などの協力会社の従業員の立入制限手続きが確立されている。
	☐ 統制区域などすべての重要施設に監視装置が設置されている。
	☐ カメラ、モバイル付カメラ、カメラ付製造装置、USB・電子記録媒体等営業秘密窃取装置の持ち込みが統制されている。

通信セキュリティ	☐ サーバ及びデータベースのセキュリティ設定を定期的に(半期以上)点検し、措置している。
	☐ 個人携帯PCや電子的記録媒体の使用・管理手順が定められ、秘密用として登録されたメモリのみ使用可能。
	☐ 営業秘密はセキュリティ措置なしに電子メールで発送できないように社規で定め、発送容量を制限している。
	☐ パスワードは3ヶ月基準で変更し、点検している。
	☐ スクリーンプロテクターに暗証番号が設定されており、離席すると自動的に動作するように設定されている。
	☐ 内部営業秘密保管サーバと外部ネットワークが区分されており、外部から内部ネットワークへのアクセスには認証が必要。
	☐ ログを記録し、営業秘密情報を保管している。

第 3 章 管理体制整備のステップ2 - 営業秘密情報の洗い出し及び重要度の区分

1. 営業秘密情報の洗い出し

1.1 競合他社に比べて強みとなる情報の把握

自社が保有している情報の内容を把握した上で、把握された情報のうち競合他社に比べて自社の強みとなる情報を把握する。

具体的には、企業競争力の基盤となる製品やサービスを特定し、それを引き出す企業業務の各プロセス、すなわち生産、販売、その他企業活動等において重要な情報を分析することにより、自社の強みとなる情報を把握することができる。

1.2 営業秘密として管理する情報の特定

また、自社が強みを持っている情報を抽出した上で、当該情報を特許権等排他的権利を確保するために出願するのか、それとも自社の優位性を確保するために営業秘密として管理するのかを判断する必要がある。

例えば、入手した製品のリバースエンジニアリングを介して比較的容易に知り得る情報（機構の内部構造など）については、営業秘密として保護するより特許権を取得した方が有利である。また、リバースエンジニアリングを介して容易に知り得ることはできないが、一旦情報の内容を入手すると容易に類似製品を生産できるような情報（製品検査工程、成分配合比率等）については、特許権を取得するより営業秘密として管理する方が望ましい。

1.3 情報の分類

また、営業秘密として管理する情報を特定した後は、営業秘密リストを作成する。営業秘密リストをデータベース化することは、以後の営業秘密管理体系を構築する上で大前提となり、会社所属の構成員に営業秘密の概念と管理の必要性を喚起させる上で重要である。

営業秘密リストを作成するに当たっては、当該情報を技術上の情報と営業上の情報に分類してそれぞれリストを作成しても良い。ここで、技術上の情報とは、工業技術に使われるすべての技術をいうものであり、経営上の情報とは、顧客名簿、顧客の管理方法、財務管理技法等を意味する。各分類によって必要となる管理体系の水準や人的・物理的措置が異なってくるので、営業秘密をその種類に応じて適切に区分して整理することは、今後の管理体系の構築において重要な意味を持つ。

また、自社が保有している営業秘密を分類してリストを作成する際には、当該営業秘密をどのような形で保有しているのかを把握することが営業秘密保護体系のうち物理的措置の立案に役立つ。

例えば、営業秘密の保有形態を、書類、記録媒体、パソコン、サーバ、ネットワーク等

に整理しておけば、営業秘密保護体系を構成する際に、各営業秘密毎に特定の物理的措置を設定(通信セキュリティ、パソコンセキュリティ、統制区域の設定等)することに役立つ。

2. 重要度の区分

前述のように、企業が保有する情報をすべて営業秘密として保護することは、莫大な人的・物的資源の浪費につながる。

したがって、営業秘密として管理されなければならない情報が膨大であり、各情報ごとに重要性に差がある場合には、各営業秘密ごとにその重要性に応じて等級をつけ、異なる水準の管理体系を構築することが望ましい。

等級算定時には、営業秘密として特定された各情報について、①当該情報の創出及び維持費用、②算出情報の水準、③情報活力度、④内部活用効果、⑤外部流出危険の5つの要素を評価して配点した後、評価点数の順で営業秘密等級をつけることができる。

例えば、以下のように「極秘」、「秘密」及び「社外秘」の3段階に営業秘密の等級をつけ、各等級によって異なる管理水準を適用することができる。

[表20]

極秘	経営において極めて重要かつごく限られた関係者のみが見ることができる情報
秘密	極秘に該当するほど重要な情報ではないが、その情報の組合せによって企業の経営に大きな脅威となり得る情報
社外秘	一般的な情報であるが、外部流出時に悪用の恐れがある情報

ただし、「極秘」に分類される情報があまりにも膨大になると、管理コストが上昇し、実効性が低下することになるため、営業秘密と特定された情報は基本的に「秘密」に分類し、その中で重要度の極めて高い一部の情報のみを「極秘」に設定することが望ましい。また、その特性上、変更が頻繁であり、アクセス可能な社員の範囲を制限することが望ましくない情報については、「社外秘」として設定することが望ましい。

第 4 章 管理体制整備のステップ 3—管理体制の整備

1. 担当部門・担当者の設置

管理体系の構築のためには、営業秘密保護管理の基本方針を文書化し、それを実現するための具体的な実施計画を設定する必要がある。また、設定された管理方針に準じて、具体的な物理的措置、人的管理を実行するための管理部門と管理責任者を選任し、その地位及び権限を具体的に文書化する必要がある。

管理部門の担当者は、営業秘密保護体系の物理的措置及び人的管理等の各部門の実務を担当する。そして、管理責任者は、営業秘密管理の実効性を担保するため、管理部分の担当者の任務実施状況を周期的にチェックし、可能な限り定期的に内部点検を行う。そして、点検の結果、潜在的な問題を発見した場合、点検項目と対象を再検討し、これを補完する。また、定期的に全従業員に対して教育研修等を行い、営業秘密管理方法と手順を従業員に周知させることが望ましい。

一方、韓国内の営業秘密侵害事例がほとんど内部者を通じて発生しているという点を考慮すると、日系企業の韓国国内支社や事業所などについては、可能な限り本社職員が営業秘密管理責任者となり、韓国人スタッフを担当者に任命することが望ましい。ここで、管理責任者は持続的な点検及び教育の主体となることとし、一般的な管理業務は韓国人担当者に一任することが望ましい。

また、韓国国内で営業秘密流出動機の大部分を占めるのが金銭的誘惑や個人営利(78%、2014年技術流出統計)であるという点を考慮すると、韓国人職員が管理責任者に選任された場合には、別途のインセンティブ提供などにより、退社時に在職中に知り得た機密流出禁止などのセキュリティ措置を実施することが望ましい。

-実際の事例（ソウル中央地方法院 2008. 3. 19. 2007カ合3903決定）

A社は、該当業務に関連する文書、ファイルなど各種資料を営業秘密として管理するためにセキュリティ規定を策定し、内容が公開されることで会社の利益を害するおそれのある秘密を、その重要性によって「重要秘」又は「社外秘」に分類して管理し、業務上直接関連のある者のみ文書や資料にアクセスできるようにし、秘密の複製、搬出、個人の保管等を禁止した。

また、セキュリティ担当官を任命してセキュリティ業務を専門担当させ、部署内のセキュリティ責任者を任命し、職員に対して随時セキュリティ教育とセキュリティ点検を実施する。

2. 人的(従業員、退職者など)管理

これまで韓国で蓄積されてきた判例の内容を検討すると、営業秘密の認定要件の中で秘密管理性を認めるにあたり、制度的システムや物理的措置に比べて人的管理をどのようにしたかを圧倒的に考慮している。これは人的管理の場合、その内容がほとんど文書化されており、当事者の義務を規定した契約の形態を持っているため、立証が容易であり、その法的効力を認めやすいからである。したがって、営業秘密保護体系においては人的管理の

重要性が最も大きいといえる。

2.1 入社時の管理

営業秘密と直接関連のある研究・開発部署及び営業秘密管理職員に対しては、入社時に営業秘密遵守誓約書と、転職及び退職時に使用・公開禁止及び競業禁止誓約書を徴求しなければならない。このような誓約書には、①対象となる情報の範囲、②秘密保護義務及び付随義務、③例外規定、④秘密保護期間、⑤在職時に創出した営業秘密の所有権帰属主体、⑥違反時の措置などが含まれ得る。

一方、新規職員が職務経験者である場合に、当該職員が自発的に前職の営業秘密を転職後に漏洩する場合、営業秘密侵害で提訴されることがあり得る。したがって、職務経験者の採用にあたっては、前職在職時に結んだ営業秘密保護契約や競業禁止契約の内容を確認し、前職で営業秘密流出に関して警告措置を受けた例があるかどうかを確認する必要がある。

また、より望ましくは職務経験者の採用時、他社の営業秘密を承諾なしに自社内で公開又は使用しないよう誓約書を受け取っておくことが望ましい。上記の誓約書の存在は、将来的に営業秘密侵害で提訴される場合に重大な過失がないことを立証する証拠になり得る。

一方、誓約書を受け取った場合でも、依然として営業秘密流出の恐れがあると判断する場合、採用後一定期間は、前職と関連のない業務を任せ、リスクを下げる必要がある。

また、採用した職員が前職の営業秘密を使用していることが確認された場合、それ以降の使用行為は悪意による営業秘密侵害行為となり得るため、直ちに使用を中止させなければならない。

2.2 在職中の管理

韓国の場合、日本と異なり、社内業務の転換を通じて事務職と技術職の間で転換が頻繁に行われており、重要なコア事業の場合、社内各部署の人材を招集してプロジェクトチームの形態で短期間運用されることが多い。

したがって、セキュリティ課題に分類された研究開発を行う参与研究員に対しては、入社時に受けた営業秘密遵守誓約書に加えて、当該プロジェクトに係る別途の秘密取扱認可を受けておくことが望ましい。

また、プロジェクトに参加した研究員に対しては、その内容を人事カード等に記録し、当該研究員の転職や退職時に営業秘密保護措置を行うのに活用するものとする。

一方、韓国において在職者又は退職者による営業秘密流出事例を見ると、他社の懐柔による営業秘密流出の割合が40%以上を占めている。したがって、在職者による営業秘密流出を事前に防ぐためには、競合他社に比べ在職者の勤務環境を改善し、業務成果に対する強力な報奨体系の確立が重要である。

より具体的には、製品の構想段階から量産段階に至るまで段階ごとに報奨体系を確立し、技術開発の初期時点よりは量産時点に至ったときに報奨額を大きくすることがより望ましい。

2.3 退職者の管理

韓国での侵害事例を見ると、在職者によって侵害発生した割合(32.9%)より、退職者によって発生した場合(72.9%)がはるかに高い。韓国の場合、1997年のIMF通貨危機以来、産業構造や労働環境が変化し、勤労者集団の忠誠度が弱まり、企業間労働人材の移動性が強化されてきた。従って、退職者に対しても、在職中の従業員に準じて営業秘密保護義務を課す仕組みを構築する必要がある。

特に退職時には、退職者が勤務当時に接した情報の範囲を容易に確認できるため、入社当時に比べ保護義務が認められる営業秘密の範疇を特定しやすい。したがって、将来的に営業秘密流出による法的措置を取る際により有利になるよう、退職者に対しては、入社時に受け取った営業秘密保護誓約書とは別に、保護義務のある営業秘密の種類を特定した営業秘密保護誓約書を受け取っておくのが望ましい。そして、在職中に管理していた営業秘密関連書類と、業務用パソコン及び資料をすべて返却するようにし、退職者が使用していた社内イントラネットIDと電子メールIDは直ちに削除しなければならない。

一方、退職者に対しては、営業秘密流出防止のため、類似の職種に対する再就職を禁ずる競業禁止義務を課すことができる。

韓国大法院の判例⁴⁴によると、競業禁止約定がない場合も、侵害行為の禁止又は予防のため退職者に競業禁止措置を取ることができるとしている。ただし、判例によると、当事者間で具体的な競業禁止約定の存在が認められない場合、会社の営業秘密を保護するため競業を禁止させる必要があるかどうかは、より慎重に判断しなければならない⁴⁵としているので、競業禁止義務をより確実に課するためには、文書化された誓約書を締結するのが望ましい。

一方、競業禁止約定の有効性に関して、韓国大法院は、勤労者の職業選択の自由と労働権保護の観点から、合理的範囲内の競業制限でなければ、その有効性を認めることができず、その有効性の判断は、①競業禁止約定によって制限対象となる職種の範囲、期間、場所、制限の対価、②使用者の利益及び③公共の利益という3つの観点から判断することとしている⁴⁶。

したがって、競業禁止約定を結びながら、過度に長期間の再就職を制限⁴⁷したり、制限される職種の範囲を過度に広く設定⁴⁸する場合には、有効性が否定されるおそれがあるので、留意しなければならない。

また、競業禁止期間の起算点については議論があるが、大法院では特別な事情がない限り、従業員の退職時を起算点としている。

⁴⁴ 大法院2003. 7. 16. 2002マ4380決定

⁴⁵ 水原地方法院城南支院2018. 11. 26. 2018カ合50314決定

⁴⁶ 大法院2010. 3. 11. 宣告2009ディ82244判決

⁴⁷ ソウル高等法院2011. 08. 01. 2010ラ384決定[仮処分異議]では、5年の競業禁止期限は、過度に職業選択の自由を制限するものだと判示した。

⁴⁸ ソウル中央地方法院 2018. 11. 1. 宣告2017ガ合559836判決

2.4 外国人職員の管理

外国人職員の場合、韓国人職員と比べて相対的に重要な技術や情報にアクセスする業務を担当する場合が多く、相対的に企業に対する所属意識が薄いため、営業秘密の流出リスクが相対的に高い。

したがって、外国人職員に対して英文の秘密保持義務誓約書を受けとっておき、継続的に点検及び教育を行う必要がある。

また、韓国にある支社については、セキュリティ責任を担当する責任者はなるべく日本人を選任し、実務担当者に韓国人を選抜することがより望ましい。

2.5 教育

会社構成員のセキュリティ意識を養うためには、入社から退職まで全社員に対する営業秘密及びセキュリティ教育を継続的に実施する必要がある。

このような教育は通常、社内営業秘密担当部署で行うことになるが、内部人材が十分でない場合は、外部講師を招聘したり、営業秘密保護センターから提供するサービス(教育用動画など)などを積極的に活用する必要がある。

一方、教育終了後は、修了証を発行したり出席者の署名を受けたりするなど、教育が周期的に行われた事実を記録に残しておく必要がある。この場合、後で営業秘密流出による法的紛争が発生しても、会社が営業秘密保護のために相当の努力(秘密管理性)をしたという点を立証する証拠となり得る。

-実際の事例(大邱地方法院2005ガ合4332判決)

- ① A社の下記のような人的管理システムが認められ秘密管理性が認められた事件
- ② 営業秘密を維持、管理するために、職員に対して本件の機械及び設備ラインの部品、設計図面、製作プログラムなどを外部に流出しないようにする。
- ③ 社員に対して、営業秘密と関連技術情報など営業秘密について、在職中はもちろん退職後も秘密を遵守し、もしこれに違反した場合は、民事・刑事上の全ての責任を負うという内容の誓約書を請求する。
- ④ 取引先や外注業者に対しても、機械及び設備ラインの製作を依頼しながら、その設計図面及びプログラム等を外部に流出する場合、一切の民事・刑事上の責任を負うという内容の誓約書を交付する。

3. 物的(執務室、生産現場、パソコンなど)管理

3.1 統制区域の設定

生産現場、勤務室などの位置や特性を考慮して統制区域を設定できる。統制区域を設定する際には、取り扱う秘密の種類、量、施設の重要度に応じて、①共用区域、②一般区域、③制限区域及び④統制区域と設定し、重要施設は制限区域又は統制区域と設定し、設定さ

れた区域ごとに管理体系を別途構成する必要がある。

一方、各区域では、設定された区域の種類を表示することが望ましいが、施設の特性によっては、制限区域や統制区域を表示しないことがセキュリティ上有利となることもある。

3.2 勤務室の管理

韓国における営業秘密の流出形態を見ると、書類、図面の窃取が最も多く、電子メール等を利用したインターネット転送による流出、保存媒体による流出がそれに続いた。すなわち、韓国における営業秘密の流出は、営業秘密が記載された書類にアクセスが容易で、パソコンを活用しやすい勤務室で主に行われていることが分かる。したがって、勤務室からの営業秘密の流出を防止する管理体系を確実に構築することが重要である。

(1) 立入制限

職員に対しては、出勤時から社員証を規定の位置に着用するようにし、協力会社の職員、情報システム部の補修などの目的で定期立入する者に対しては、社員証とは異なる色の定期入館証を携帯するようにする。また、外部立入者は社内立入時に必ず事前予約するようにし、立入時の人的事項、目的、訪問対象職員などを記載するようにする。そして、臨時立入者についても社員証とは異なる色の臨時入館証を携帯するようにする。

一方、複数の勤務室の一部をその重要度に応じて統制区域として設定した場合、統制区域への立入者数を制限するため、社員証、定期入館証等に電子チップを組み込んだり、立入可能な区域によって入館証の色を別にする必要がある。

(2) 書類の管理

保管:営業秘密が記載された書類については、スタンプを押したりステッカーを貼ったりする方法等により秘密として管理される情報である旨を表示した後、少なくとも一般文書と切り離して二重に施錠装置が施された別途のキャビネット等に保管する。また、分離又は離脱可能な記録物は、総ページと一連番号を付記して、分離又は離脱から保護する。

搬出及び複製:営業秘密が記載された書類を搬出する際は、必ず部署長の許可を得るようにして、任意搬出を禁止する。書類の複製の際は、原本や別の記録台帳に複写日時、部数、配布先等を記載することを義務付ける。

回収及び廃棄:営業秘密が記載された書類については、復元できないよう完全に破碎し、複製本についても使用後は直ちに回収し、破棄することが望ましい。

(3) 電子媒体の管理

保管:USB等の記録媒体の場合、記録媒体自体にステッカーを貼付したり、営業秘密である旨を表示するデータを電子情報そのものに入れて、秘密として管理される情報である旨を表示する。また、書類と同様に、記録媒体自体も二重に装置が施錠された別のキャビネット等に保管する。

搬出及び複製: 記録媒体に保存されたファイルについてはパスワードを設定する。より望ましくは、外部へ物理的に搬出できる記録媒体に情報を記録するよりも、ファイアウォールを有する自社サーバに記録し、一定の資格を有する内部者又は外部者がサーバを介して当該情報にアクセスできるようにする。そして、電子情報を書類で印刷出力する際には、ICカードと複合機とを連動させることにより、利用者及び印刷枚数を管理することが望ましい。

回収及び廃棄: 営業秘密の電子データを使用・保管していたコンピュータ・サーバ等を廃棄する場合、データ復元が不可能になるように物理的な破棄を原則とし、記録媒体を再使用する際は、データを完全削除、フォーマット及び磁気消去後、再使用する。

3.3 生産現場の管理

(1) 勤務者の管理

携帯電話又はその部品などの小型製品の場合、研究開発のための試作品やサンプルを生産する生産ライン上で窃取した後、携帯して帰宅することで外部に流出するケースが多い。したがって、生産ラインへ出退勤する勤務者に対しては、手ぶら通勤を原則とする必要があり、出入口でこれを検査できる検査台を備えることが望ましい。

また、最近では、携帯電話を利用して生産ラインを無断で撮影した後、SNSなどを通じて外部に流出するケースが増えている。したがって、出退勤時に勤務者の携帯電話のカメラにはセキュリティステッカーを貼付させたり、現場でのカメラの作動、外部SNSへのアクセスなどを制限するセキュリティソフトウェアのインストールを義務付ける必要がある。

(2) 工場見学など外部立入者の管理

製品紹介・購買相談・工場見学などで企業を訪れる外部者も、相談又は見学過程で知り得た営業秘密を流出するおそれがある。したがって、工場見学の際にも、重要施設へのアクセスができないようにその動線を制限する必要がある。

一部外者による見学時に制限措置が行われず、秘密管理性を否定した外国の事例韓国内の事例ではなく、米国での営業秘密の紛争事例⁴⁹で、営業秘密だと主張する製造ラインにおいて定期的な見学を実施し、見学ルートに営業秘密だという表示もなかった場合、そして見学者に何の注意も払わず、専門雑誌に取材されて写真撮影まで行われた場合に対し、秘密管理性が否定された。

3.4 コンピュータの管理

(1) 個人パソコンのセキュリティ管理

⁴⁹ Motorola, Inc v. Fairchild Camera and Instrument Corporation et al. (1973)

職員がオフィスで使用するパソコンについては、ステッカーを貼り、取扱者及び管理責任者を指定し、周期的に点検する。一方、最近では、企業内部者の関与なしに、ランサムウェアや標的型攻撃メールといったサイバー攻撃により企業が保有している技術情報や営業情報を奪取する行為が新たな侵害類型として現れている。したがって、上記の侵害行為から営業秘密の流出を防止するため、次のような事項に留意する必要がある。

- パソコンセキュリティ用ソフトウェアのインストール
- ライセンスのない違法ソフトウェアの使用禁止
- ID及びパスワードの設定及び周期的な変更
- 個人パソコン別のスクリーンセーバー及び専用パスワードを使用(スクリーンセーバーの作動時間を20分前後に設定)
- ワクチンプログラムを利用して周期的に点検し、OSのセキュリティアップデートを迅速に実行
- パソコン内の重要文書については照会ができないように暗号化し、別のデータベースに保存

(2) 携帯用パソコンの管理

認可されていない個人用ノートパソコンの使用を禁止し、持ち運びできるノートパソコン内のハードディスクへの重要情報の保存を禁止する。また、業務上の目的で重要ファイルを保存する際には、必ずファイルごとにパスワードを設定するようにする。ノートパソコンの外部搬出時には部署長の認可を受けるようにし、搬出内訳は別途台帳に記録する。

また、パソコンには認証機能や遠隔操作によるデータ消去機能を付加するのが望ましい。

望ましくは、携帯用パソコンは端末の機能のみを行えるようにし、重要な業務やデータのアクセスは、通信セキュリティの整った社内サーバに接続して行われるようにする。

3.5 通信セキュリティ

(1) 情報管理システムの構築

持ち運びができる記録媒体や書類等は容易に外部流出するため、重要情報については、記録媒体や書類に記録するよりも、イントラネットを通じてのみアクセス可能な社内サーバに保存することが望ましい。

また、個人パソコンを中央統制型ネットワーク端末に取り替え、職員のすべてのファイルを中央で統制しながら、職員の情報アクセス記録を管理することが望ましい。

また、DRM(Digital Rights Management)システム、統合認証権限管理(Extranet Access Management)システム及び知識管理システム(Knowledge Management System)を導入し、外部からの企業のイントラネットへのアクセスを制限し、資料にアクセス可能なユーザの範囲を制限する一方、情報流出の際に流布者を追跡できるようにするシステムを構築することが望ましい。

(2) Eメールセキュリティ管理

電子メールは業務上頻繁に使用され、前述のように、電子メールによる営業秘密の流出が2番目に多いことを考慮すると、以下のような使用指針を設定し、順守することが重要である。

- 外部発送Eメールの容量を制限し、これを超過したファイルを発送する場合は部署長の認可を受ける。
- 転送先が不明な電子メールに対しては削除を優先し、閲覧時にはウイルス検査を先に実施する。
- 業務目的以外の会社の電子メールの使用を禁止し、メールにファイルを添付する際には必ずパスワードを設定する。

(3) その他

電子メールやサーバなどと比較して、FAXや電話などはセキュリティが極めて脆弱な手段である。したがって、FAXでの重要内容の送付を禁止し、FAXを通じた送信リストを定期的に確認する。やむを得ずFAXで機密文書を送付する際には、FAX用紙にセキュリティレベル(「極秘」、「対外秘」等)を押印し、部署長の承認を得た上で発送する。

また、社内に設置された電話については、通話内容が録音されるようにし、これを定期的に点検する。

-実際の事例(ソウル中央地方法院2008. 3. 19. ザ2007カ合3903決定)

A社は、情報セキュリティシステムに関して、ファイアウォールの設置、電子決済システムの導入、ウェブキーパー及びメールロギングシステムの構築、統合認証システムの構築、電子文書管理システムの全社適用など電算システム関連の技術的セキュリティを強化し、外部者の立ち入り統制のためのセキュリティゲートの設置、IDカードの使用など物理的立ち入り統制システムも運営した。

4. 取引先(部外者、ライセンシーなど)の管理

4.1 取引先の管理

取引契約上の相手方が、契約成立前の交渉段階で相手方の持っている営業秘密の価値を評価するために情報開示を求める場合が多い。しかし、技術契約段階のうち、交渉段階で技術流出が最も多く発生することを考慮すると、契約が決裂する場合に備え、交渉過程では重要情報を相手方に提供することには気をつける必要がある。

また、交渉が完了して契約段階に至れば、契約書内に、営業秘密の目的外の使用禁止、第三者に対する開示禁止及び秘密管理保持義務を契約書上に明記する必要がある。ただし、契約書上に過度な営業秘密保護義務を課すことになれば、契約相手としては、事業を営むために営業秘密を活用するにあたり、過度な制約を受けることになり、その結果、秘密保

持義務を順守できなくなる原因となりうる。また、いずれか一方に契約内容があまりにも不合理な場合、民法に基づいて契約を無効化することもありうる。

したがって、契約書上には、秘密保持が必要な情報の範囲、第三者に対する開示の範囲等を合理的に設定する必要がある。また、契約一方の営業秘密を使用する他方の立場から、法的紛争の余地を残さないためには、営業秘密の範囲と使用目的、開示範囲などを具体的に限定する必要がある。

また、取引先への製品紹介、購買相談、工場見学などを理由に訪問、あるいは企業間の合併やそれに先立つ実査時、共同開発事業の検討開始などのように、契約の成立や企業間協力プロジェクトの実施のために企業の内部情報を開示しなければならない過程において、企業内部の営業秘密が漏えいする事例が多い。したがって、このような場合、訪問者の見学コースを指定し、提供される技術資料や広報パンフレット等についてセキュリティ検討を事前に行うなど、営業秘密漏えい防止対策を講じる必要がある。

また、各種政府機関及び自治体等の関係機関に研究費又は研究プロジェクト獲得のための情報提供の際に通常一般文書で提供し、関連内容が漏えいする事例がある。したがって、政府機関等に資料を提供する際にも、提供時の表紙にセキュリティ等級を表示し、当該機関に対して社外秘に準じて取り扱うことを求める必要がある。

また、コンサルタント、顧問弁護士、会計士などの業種については、法で秘密保持業務が明示されているが、別途秘密保持契約書を締結しておいた方がより安全である。特に、下記の事例のように、当該人達の場合、業務遂行の過程で企業秘密を知り得る機会が多いにもかかわらず、会社からの拘束を受けることが少ないため、秘密漏えいのリスクが常に存在することに留意する必要がある。

－ 専担弁護士が個人の携帯電話で技術資料を無断撮影した事例

- ・A社はセキュリティ点検のためCCTVを確認していたところ、特許登録相談のため企業を訪問した専担弁護士が会社の機械図面をスマートフォンで無断撮影した事実を確認。
- ・A社は専担弁護士と長年取引をしており、秘密保持誓約は別途受けていない
- ・A社は内容証明を通じて弁護士の秘密保持義務について告知し、弁護士の携帯電話から無断撮影した写真の削除措置をとった。

4.2 協力会社などの管理

協力会社は多数の同種企業を相手にしているため、特定企業に対する連帯意識が弱く、多様な情報に触れることができる位置にあって、不正な目的を持って営業秘密を流出しようとする場合、その実行が非常に容易である。

特に、韓国における営業秘密流出企業の形態を見ると、中小企業による奪取の場合(75.6%)が、その他の場合(国内大手、中堅企業等)に比べて非常に高いことが示されている。中小企業の場合、人的・物的資源の限界から営業秘密に係るセキュリティ教育や保護体制が十分に整っていない場合が多いため、特に中小企業と取引を行う場合、営業秘密が流出しないようさらに留意する必要がある。

したがって、協力会社に対しては、契約の終了後も一定期間秘密保持義務を課す内容の

特約を結ぶ必要がある。

特に、協力会社の点検過程で新製品モデル、設計図面などを無断でコピーし、保管していたことが摘発された事例が多数ある。したがって、協力会社と共同での業務遂行時は、企業間はもちろん、実務者とも必ず秘密保護誓約書を徴求しなければならない。

－ 企業間取引時の営業秘密流出事例

(1) 請け取引関係を利用して確保した中小企業の技術を系列会社は無断で流出
中小企業B社は、通信機器自動開閉装置を自社開発して大企業A社に納品したが、まもなくA社は予告もなく取引中断を通知。
以後、大企業A社は系列会社を通じてB社が提供した技術を利用して製品を生産した後、これらの納品を受け、B社は営業ができなくなり不渡りとなった。

(2) 協力中小企業の技術を奪取して、下請代金の引下げに利用
大企業C社は、独自技術を開発したD社の製品性能を認めて契約を締結したが、納品条件としてD社の技術提供を要請し、D社は取引断絶を懸念して核心技術を同時に提供。
以後、大企業C社はD社の技術を他の中小企業に提供・開発した後、価格競争を誘導し、D社は納品価格を大幅に引下げざるを得なかった。

(3) 中小企業との共同技術開発過程において技術を奪取した後、独自に製品開発
ソフトウェアを開発するF社は、大企業E社との共同研究開発を進める過程で大企業の担当者から核心技術の提供を要求され一切の資料を提供したが、C社は内部事情などを理由に突然共同技術開発を中断。
暫くした後、大企業はF社の核心技術を利用して当初共同開発しようとしていた新製品を発売、F社は共同研究開発ときに技術資料の使用契約書を作成せず、技術奪取による被害をこうむった。

5. テレワークの実施に伴う管理上の留意点

物的営業秘密保護の仕組みが整った社内勤務環境とは異なり、テレワークという業務環境は、業務当事者による営業秘密流出以外にも、ネットワーク犯罪等による第三者の侵害行為にも脆弱である。

従って、ユーザはテレワーク時のセキュリティ強化のための社内イントラネット接続システムやソリューションを補強する必要があり、テレワーク勤務者に対しては、以下の服

- ① セキュリティ維持のための一般原則を遵守すること
- ② 会社の営業秘密に関する文書作業は自宅内でのみ行うこと

⁵⁰ キム・ギョンテ「第4次産業革命時代の労働条件規律-スマートワーク勤労者を中心に」

- ③ ランサムウェア、スパイウェア等の悪性コードに感染しないように必要なすべての措置を講じること
- ④ 業務関連の資料は、作業終了後すぐに会社のクラウドサーバーに移し、勤労者の個人スマート機器から完全に削除すること
- ⑤ 公開場所において公衆無線LANのような開放型無線通信網に接続しないこと
- ⑥ 自宅でも独立作業スペースを確保し、ロック機能を備えること

一方、原則として営業秘密は他の文書とは区別し、社内で定められたロッカーに保管、あるいはアクセス制限措置がとられた情報システムに保管する。しかし、在宅勤務中に職員が意図的に、又は無意識に家の個人コンピュータに会社の資料を保管する場合がある。

しかし、在宅勤務者も自分のコンピュータに保存されている会社の営業秘密を無断で利用する権限はなく、これに違反した場合、以下の事例のように犯罪行為に該当することもある。したがってこのような問題を解決するためには、例えば在宅勤務時には、社内に備えられた自身のコンピュータに外部接続(リモートデスクトップ等)を介して作業が行われるように制限し、家のコンピュータから直接社内営業秘密にアクセスすることを制限することを考慮に入れても良い。

-在宅勤務中に会社の機密情報を自分のコンピュータに保存して私的流用した事例(大法院2008. 7. 24. 宣告2007ド11409判決)

在宅勤務中のAは、海外商品の購買を代行するショッピングモール会社のB社に入社してセキュリティ誓約書を作成し、ウェブサイト管理者及びユーザーモードに対するプログラムを開発した。自宅で会社のサーバに接続して作業を行った後、自宅にあるコンピュータにソースファイルなどのデータを保存した。その後、AはB社が賃金を遅滞すると退職し、別の商号で事業者登録を済まし、自分のコンピュータに保管されていたソースファイルを修正・補完し、ショッピングモールのウェブサイトを開発、購買代行サービス事業を開始した。しかし、AはB社の営業秘密を取得、使用したことを理由に検察によって営業秘密保護法違反の疑いで起訴され、有罪判決を受けた。

6. 営業秘密の原本証明サービス、技術任置サービスによる管理

6.1 営業秘密原本証明サービスによる管理

上記の営業秘密管理体系の構築にもかかわらず、営業秘密が外部に流出した場合、それ以降に行われる民事訴訟等において、営業秘密の存在及び保有時点を立証することは容易ではない。

この場合、営業秘密保護センターから提供する原本証明サービスを利用して、あらかじめ当該営業秘密の保有事実及び保有時点について公的な確認を受けておけば、以後訴訟が進行する場合において立証責任が緩和される。

しかし、原本証明サービスは、原本の存在と保有時点のみを公証するための制度である

ため、営業秘密自体の管理や流出防止の責任は、依然として営業秘密保有企業が負う。

また、営業秘密が記載された電子文書の管理に問題が生じ、ハッシュコード値が変われば、原本証明が不可となるので、当該電子文書の内容が変更されないように綿密に管理することが重要である。

6.2 技術資料任置サービスによる管理

上記の営業秘密管理体系の構築にもかかわらず、下請契約の受託企業の場合、取引上優位にある委託企業から不当に営業秘密に該当する情報を交付することを求められる場合には、これを回避することは容易ではない。

この場合、技術資料任置制度任置サービスを利用し、大・中小企業・農漁業協力財団の技術任置センターに営業秘密を任置した上で、契約手続により、技術任置センターから委託企業に当該営業秘密を交付するようにすることができる。

ただし、技術任置センターに任置された営業秘密についても、受託企業が同意した場合、委託企業に交付が可能であるため、その後、委託企業が契約上優越した位置を利用して交付を強要する場合、これを拒否することは容易ではない。

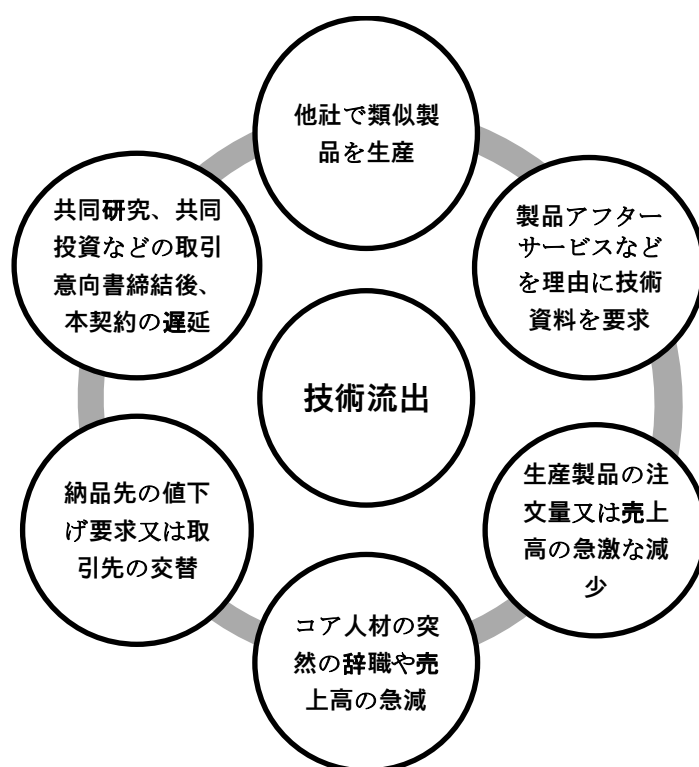
したがって、技術資料任置サービスを利用する場合においても、委託企業と受託企業との間の秘密保持契約書等により、交付可能な情報の範囲及び使用目的と開示範囲を明確にすることが重要である。

第 5 章 漏洩時の対応

1. 漏えいの兆候

1.1 技術流出の兆候

競合他社や取引先に関して、下記のような急激な変化が感知されたり、内部要因とは無関係に売上高の急激な変化が感知された場合、技術流出が発生した可能性がある判断できる。



1.2 産業スパイの識別要領

社内職員又は訪問者の挙動に関して以下のような疑わしい状況が発見される場合、当事者が産業スパイである可能性を排除できないため、注意観察する必要がある。

- (1) 本人の業務と関係のない他の職員の業務について随時質問する者
- (2) デジタルカメラ等業務と関係のない機器を事務室に搬入する者
- (3) 本人の業務と関係のない他の部署の事務室に頻繁に出入りする者
- (4) 研究室等機密保管場所等に自らの業務とは無関係に出入りを試みる者
- (5) 普段と違い同僚との接触を回避するなど最近情緒変化が激しい者
- (6) 主要部署で働いていたのに理由もなく急に辞職を望む者
- (7) 業務にかこつけて重要機密資料をコピー、個人的に保管する者

- (8) 特別な事由なく、業務終了後や祝日に事務室によく一人で残っている者
- (9) 技術習得よりコア技術者等との親交に関心がある研修生
- (10) 自分の住居地に同僚が訪問することを過度に避ける研究員
- (11) 研究活動よりも研究成果物の確保に過度に執着する研究員
- (12) 視察・見学において、指定されたコース以外の施設に関心を持っている訪問客

第3章の「1. 営業秘密の侵害類型別統計」で示されたように、韓国における営業秘密流出の主体は、内部者が外部者より2倍以上多く、また内部者の場合、退職者の割合が高かった。

したがって、従業員が退職前に上記のような異常行動を見せた際は、退職後又は在職中に営業秘密の流出が発生する可能性が高いとみなし、注視する必要がある。

例えば、従業員が普段と違って職場の同僚との接触を避けたり、同僚との頻繁な摩擦が発生したりするなど、情緒の変化が激しい場合は、周囲から気を使って見守る必要がある。また、このような社員が急に退社をすることになった場合、退社後の競合他社入社などその挙動を注意深くチェックする必要がある。

また、従業員が秘密情報を保管しているサーバや記録媒体等にアクセスする回数が急に増えたり、業務を理由に機密資料をコピーして個人的に保管するケースを発見した場合には、やはり要注意が必要である。警察又は検察の調査において、技術流出犯の相当数が会社の機密を個人的に保管している理由を「在宅勤務」と言い繕うケースが多い。したがって、社内勤務のみならず在宅勤務時にも業務機密を個人所有媒体に保存することを厳禁とし、その定期的な確認が必要である。

2. 初動対応(紛争解決の手順とロードマップ)

2.1 流出事実の発見及び報告

流出事実が見つければ、簡単な事実関係を確認した後、企業内部の報告体系に沿って上部に直ちに報告する。

2.2 技術流出に対する独自調査

内部者によって技術が外部に流出した状況が明らかになった場合、技術流出が疑われる部署又は役職員に対する業務内訳、記録物アクセス状況(電子メール、書類、USB等の使用内訳、コア技術に対する修正履歴等)を入手し、これについて調査する。

また、外部企業へコア技術が流出したことが確認された場合、流出技術の使用が疑われる会社に対して、当該技術の開発及び発売等の動向を把握(疑いのある会社の役職員の行動等の調査)する。

2.3 追加の技術流出の防止のための応急措置の実施

社内確認の結果、侵害が探知されたり、侵害が予想される場合、関連重要文書等を回収

して追加流出を防止し、重要文書にアクセスできる会社内ネットワークを点検する一方、外部流出が疑われる外部接続ネットワーク経路、関連職員ID、電子メールの使用を遮断する。

2.4 侵害事実を立証するための証拠資料の確保

侵害現場の状況及びコンピュータのハードディスク等の関連物品を保存し、陳述書、監視カメラ撮影物、写真等を迅速に確保する。また、証拠信憑性のため、各証拠ごとに、立証しようとする内容、場所及び証拠確保の経緯等を別の文書で詳細に記録する。

(1) 被疑企業に関する資料

被疑企業や製品に対する技術説明資料、被疑企業内の 人事異動情報 など

(2) 被疑者特定のために必要な資料

被疑者の人事資料、入退社記録資料及び就業時のセキュリティ誓約書など、

(3) 被疑者の使用資料

被疑者が使っていた会社のアカウント、該当記録に関するアクセス内訳、電算ネットワークへのアクセスログ、被疑者が使用したすべてのデジタル機器(携帯電話、パソコン、USBなど)

(4) 被害技術の管理方法

被害企業の営業秘密管理方法(アクセス権、保護システム等)

(5) 流出技術の説明資料

流出した技術の機能を説明し、特定できる資料

2.5 流出への対応時に考慮すべき事項

(1) 仮処分の積極的活用

営業秘密侵害の中断を求める仮処分申請の場合、その特性上、本案訴訟より迅速に処理され(通常2週間から1ヶ月所要)、仮処分決定が下されれば、事実上侵害者は刑事処罰を恐れ、合意を先に提案してくる場合が多い。したがって、営業秘密侵害を理由とする本案訴訟に先立って仮処分を申請した方がより有利である。

(2) 訴訟よりは調停や仲裁を活用

営業秘密の侵害に係る紛争が外部に漏れることが望ましくなかったり、侵害された情報の特性上速やかな救済措置が必要な場合には、訴訟に先立って仲裁や調停制度を活用することが望ましい。後述するように、上記制度によると、コストが安く迅速かつ非公開で進むこととなるため、特にIT企業間の紛争解決においては、より有利である。

(3) 警告書簡の発送

民事・刑事上の措置又は調停、仲裁措置に先立ち、侵害者に警告書簡を内容証明郵便で発送する場合、営業秘密侵害者に対して心理的な圧迫を加え、侵害行為を暫定的に中断させることができる。

なお、警告書簡の発送以降の営業秘密侵害行為は悪意による実施に該当することとなるため、今後の損害賠償請求の際により有利な判断を受けることができる。

(4) 証拠収集に関わる刑事上の措置の活用

営業秘密侵害事件の場合、ほとんどの関連証拠が侵害者の手元にある場合が多い。しかし、韓国の場合、米国と違い、訴訟当事者の証拠提出を強制する証拠開示制度を持っていない。

民事訴訟法第344条では、このような証拠の構造的な偏在を解消するため、文書提出義務を規定しているが、同条第1項ハ目では、技術又は職業の秘密に属する事項が記載されており、これを秘密とする義務が解消されない場合には、その文書の所有者が法院の文書提出命令を拒否できるとしている。

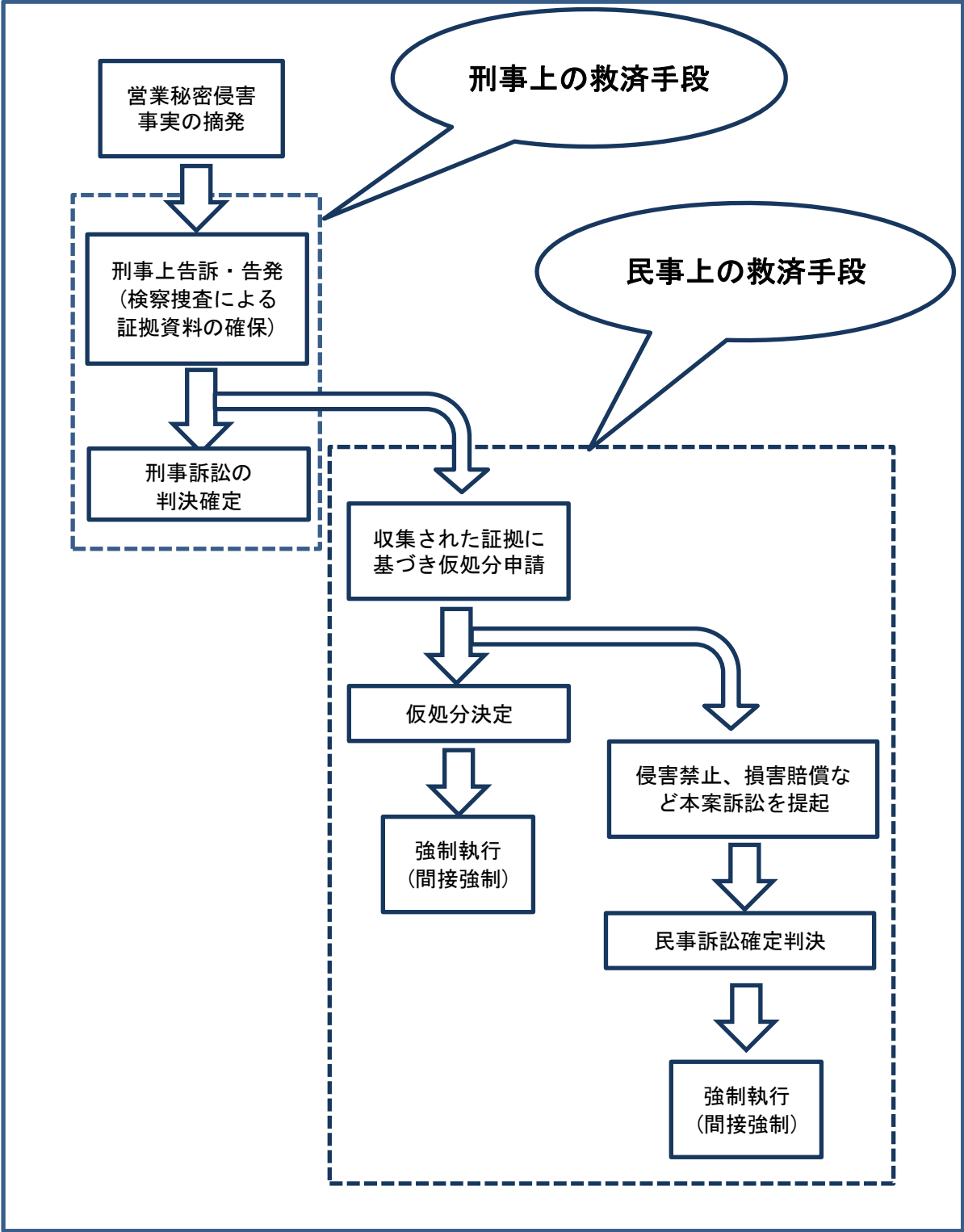
したがって、法院の文書提出命令に対し、当該文書が自社の営業秘密に属するものであることを理由に、上記民事訴訟法第344条第1項ハ目に従い侵害者が文書提出命令を拒否すれば、被害者である原告としては立証するすべがなくなり、敗訴する可能性が高い。

このような点を考慮し、民事訴訟の提起前に、刑事手続により証拠を確保し、これを利用して仮処分申請など民事訴訟を提起するケースが最近増加している。

この場合、刑事訴訟の進行状況から民事訴訟を起こすかどうかを前もって判断でき、公権力による押収捜索によって証拠を十分に確保した状態で民事訴訟を起こすことができるため、訴訟の優位を占めることができる。

ただし、刑事訴訟が遅れる場合、仮処分の時点を失期することもあり、一つの訴訟が他の訴訟に強い影響を及ぼすため、捜査の不備で刑事訴訟で敗訴する場合は、民事訴訟も敗訴となる可能性が大きくなるため、このような点に留意する必要がある。

[図] 効果的な民事上・刑事上の対応戦略



3. 民事的解決方法

営業秘密侵害行為を民法上の不法行為の特殊な形態である不正競争行為の一類型に分類し、これに対して侵害行為の禁止又は予防請求権、侵害行為により作られた物などの廃棄・除去請求権、侵害行為に対する損害賠償請求権、営業秘密保有者の信用回復請求権などを認めている。各請求権の内容は、以下のとおりである。

3.1 禁止及び予防請求権(営業秘密保護法第10条第1項)

(1) 意義及び必要性

営業秘密の保有者は、営業秘密の侵害行為をしたり、またしようとする者に対し、その行為によって営業上の利益が侵害され、又は侵害される恐れがある場合には、法院にその行為の禁止又は予防を請求することができる。

営業秘密侵害禁止及び予防は、侵害行為を禁止又は予防できる最も直接的で効果的な手段である。

(2) 当事者

(a) 請求権者

営業秘密侵害禁止請求権を行使できる者は、営業秘密の保有に関して正当な権原を有する者又は事実上の保有者である「営業秘密の保有者」が請求権者となる。具体的に例示すると次のとおりである。

- ・ 営業秘密を最初に開発した原始取得者
- ・ 譲受人、実施権者など正当な権原によって営業秘密を保有し使用する者
- ・ リバースエンジニアリングによる営業秘密の保有

米国では、リバースエンジニアリングを正当な手段による営業秘密の取得行為と認めており、韓国大法院でもモナミ事件(96ダ16605判決)でリバースエンジニアリングによる営業秘密の取得行為の正当性を間接的に認めている。したがって、リバースエンジニアリングによる営業秘密の保有者も正当な手段により営業秘密を保有する者として請求権者に該当すると見なすことができる。

(b) 侵害禁止請求の相手方

侵害禁止請求の相手方は、営業秘密を侵害する者、又は侵害しようとする者であって、侵害行為を現在行なっている者、又は着手したり、着手する可能性が高い者である。

(3) 要件

(a) 営業秘密の侵害行為(産業技術の侵害行為)

侵害禁止の対象になるのは、営業秘密保護法第2条第3号に列举された営業秘密侵害行為、

又は産業技術保護法第14条に規定する産業技術の侵害行為である。

(b) 営業秘密(産業技術)を侵害する行為又は、侵害行為をする恐れが存在
侵害禁止及び予防請求権を行使するためには、営業秘密を侵害する行為又は侵害行為をする恐れがある場合でなければならない。ここでいう「侵害行為をする恐れがある場合」とは、単純な侵害の可能性がある程度だけではならず、侵害の可能性が顕著に高い場合であるべきで、これに対する立証責任は請求権者が負う。

(c) 営業上の利益が侵害されたり、侵害される恐れが存在
侵害禁止及び予防請求権を行使するためには、実際に営業秘密侵害行為又は侵害の可能性により営業上の利益が侵害されたり、侵害される恐れが存在する場合でなければならない。ここでいう「営業上の利益」とは、営業秘密侵害行為から保護される価値のある全ての利益を意味する。

また、「営業上の利益が侵害される恐れ」とは、単純な主観的侵害の可能性だけではならず、社会通念上客観的に営業上の利益が侵害される可能性が存在しなければならない。このような事実の立証責任は、請求権者にある。

ただし、最近の下級審判例では、ひとまず相手方が不正な手段で営業秘密を取得したことが立証される場合には、特別な事情がない限りその不正取得者によって営業秘密が使用されたり、公開されて営業秘密の保有者の営業上の利益が侵害される恐れがあると見なさなければならないと判示し、立証責任を多少緩和させた。

(d) 故意・過失などの主観的要件の不存在
営業秘密侵害禁止及び予防請求権の場合、故意や過失のような主観的要件を必要としない。

従って、営業秘密や産業技術の侵害行為が善意や無過失で行なわれた場合でも、営業秘密侵害禁止及び予防請求の対象となる。

(4) 営業秘密侵害禁止

(a) 禁止行為の特定
法院は、判決として、営業秘密を侵害して製造された特定の製品の生産を一定期間中止させたり、完成した製品の配布及び販売を禁止させることができる。

一方、営業秘密侵害禁止を命じるためには、まず禁止の対象となる営業秘密が特定されなければならない。特に、営業秘密の場合には別途に登記や登録の公示のための法的制度がないため、被請求人に不測の損害が生じないように具体的に特定する必要がある。

しかしながら、営業秘密はその特性上企業が保有する他の情報と区別して具体的に特定することが容易でなく、またその侵害禁止を命じる過程において営業秘密が流出する恐れがあるため、具体的な営業秘密の特定が困難な場合が多い。

これに関する下級審判決では、判決や主文又は理由に営業秘密が具体的に指摘される場合には、この過程で営業秘密の内容が流出する恐れがあるため、他の不作為請求とともに

その対象を具体的に詳しく指摘することを要しないと判示している。

＜営業秘密侵害禁止時に対象となる営業秘密の特定と関連する判例＞

－ソウル高等法院 1996. 2. 29. 宣告 5ナ14420 判決

判決の主文及び理由に営業秘密の具体的な内容がそのまま指摘される場合、営業秘密侵害行為者に自身が侵害した営業秘密の内容を再確認することができる機会を与えるだけでなく、特定又は不特定多数の第三者が判決文を閲覧したり、これを入手してその営業秘密の内容を知るようになり、結局のところ営業秘密がこれ以上営業秘密として保持されなくなる懸念があり、これによって逆に営業秘密が侵害される素地がある。営業秘密侵害禁止を命じる判決の主文において、その営業秘密の内容は建物明渡のような他の履行判決ほど具体的に詳しく指摘されることを要しない。

一方、後述するように、2011年に改正された営業秘密保護法では、訴訟の当事者又は代理人などの訴訟過程で知った営業秘密を訴訟以外の目的で使用したり、公開する行為を制限することができるように、第14条の4ないし14条の6で秘密保持命令制度を新設し、18条の4で秘密保持命令違反時には5年以下の懲役又は5千万ウォン以下の罰金に処するようにした。

(b) 禁止期間

営業秘密侵害禁止期間は、営業秘密の侵害行為者が独自に、又はリバースエンジニアリングなどによって合法に開発するのに必要とされる期間などを考慮して判断する。したがって、営業秘密侵害者が有している技術水準、営業秘密が有している技術的水準及び営業秘密が属した技術分野の技術水準などを考慮して判断することになる。

一方、大法院判例では営業秘密の永久的な侵害禁止は制裁的な性格を持つことになるだけでなく、公共の利益と相反して認められないとしている。

＜営業秘密侵害禁止期間の算定に関する大法院の判例＞

－大法院 1996. 12. 23. 宣告 96ダ16605 判決

『営業秘密侵害行為を禁止させることは、侵害行為者がそのような侵害行為によって公正な競争者より'有利な出発(head start)'ないし'時間節約(lead time)'という優越的な位置から不当に利益を取ることができないようにし、営業秘密保有者にそのような侵害がなかったのであれば、本来いた位置に戻れるようにするところにその目的があるということであるから、営業秘密侵害行為の禁止はこのような目的を達成するのに必要な時間的範囲内において技術の急速な発達状況及び弁論に現れた侵害行為者の人的・物的施設などを考慮して侵害行為者や他の公正な競争者が独自の開発やリバースエンジニアリングのような合法的な方法によってその営業秘密を取得するのに必要な時間に相当する期間に制限しなければならず、永久的な禁止は制裁的な性格を持つことになるだけでなく、自由な競争を助長し、従業員がそれらの知識と能力を発揮することができるようにしようとする公共の利益と相反して認められない。』

(c) 禁止の起算点

侵害禁止期間の起算点がかなり前の時点である場合には、現在時点を基準に既に侵害禁止期間が経過してしまっている可能性があり、この場合、侵害禁止請求が認められなくなる。したがって、侵害禁止期間だけでなく、侵害禁止期間の起算点がいつなのかも重要である。

退職者による営業秘密侵害禁止期間の起算点については、営業秘密侵害に対する本案判決が確定する時点を起算にしなければならないという見解と、従業員の退職時を起算点に

しなければならないという見解があり、判例の立場も分かれたが、大法院1998年2月13日宣告97ダ24528判決によって退職時の説で立場が整理された。

したがって、現在の韓国大法院の立場としては、退職者による営業秘密侵害禁止請求時の起算点は、当該従業員が退職する時点といえる。

〈営業秘密侵害禁止期間が従業員の退職時から開始されたとする大法院の判決〉

—大法院 1998. 2. 13. 宣告 97ダ24528 判決

『営業秘密が保護される時間的範囲は、当事者間に営業秘密が秘密として存続する期間であるため、その期間の経過により営業秘密は当然消滅し、もはや秘密ではないと見なさなければならず、その期間は退職後の不正な目的の営業秘密侵害行為がない平穩・公然な期間のみを示すか、その起算点は退職後の新しい約定があるとき、又は営業秘密侵害行為が最後に行なわれたときか、さらには営業秘密侵害禁止期間中に営業秘密を侵害する行為を行なった場合には、侵害期間の分だけ禁止期間が延長されなければならないと見なすことはできない。』

(5) 営業秘密(産業技術)侵害の予防請求

営業秘密侵害予防請求は、現実的に侵害行為が行なわれてはいないが、将来的に侵害が発生する可能性が顕著に高い場合に認められる。

一方、「営業上の利益が侵害される恐れ」は、実行行為の着手が可能な客観的状況下で実行しようとする考えを有している場合に認められ、このような事情は予防請求をする者が立証しなければならないが、不正公開行為の場合には禁止されることによる不利益に比べて公開による被害が極めて大きいという点で、その立証の程度が緩和される。

前述のとおり、判例も、営業秘密が不正な手段で取得された事実が立証されれば、特別な事情がない限り、不正取得者によって営業秘密が使用されたり、公開され、営業秘密保有者の営業上の利益が侵害される恐れがあると見なさなければならないと判示している。

3.2 廃棄・除去等請求権(営業秘密保護法第10条第2項)

(1) 意義及び必要性

侵害禁止予防請求時には、侵害を構成した物の廃棄、侵害行為に提供された設備の除去、その他侵害行為の禁止又は予防のために必要な措置をとることを請求することができる(営業秘密保護法第10条第2項)。営業秘密侵害行為に提供された設備をそのまま保持すれば、その後も営業秘密が再び侵害される恐れが大きいからである。

(2) 廃棄請求の対象

廃棄請求の対象となるのは、侵害を構成した物又は侵害行為に提供された設備である。例えば、秘密情報が記載された設計図、仕様書・説明書、顧客名簿などや営業秘密を侵害して製造された試作品、完成品又はこのような製品を製造するための製造機械などがその対象となる。

(3) 廃棄対象物の存在の有無及び所持者特定の必要性

侵害禁止・予防請求をし、侵害を構成した物の廃棄又は除去などをともに請求する時には、該当物の現存の有無及びその物の所持者及び処分権者を明確にしなければならない。したがって、該当物が現存するのか、その物を誰が所持しているのか、そしてその物に対する処分権限が誰にあるのかが明確でないままその物の廃棄を命じる判決は違法となる。

3.3 損害賠償請求権(営業秘密保護法第11条)

故意又は過失による営業秘密侵害行為により営業秘密保有者の営業上の利益を侵害し、損害を加えた者は、その損害を賠償する責任がある。

3.4 信用回復請求権(営業秘密保護法第12条)

(1) 意義及び必要性

損害賠償は、金銭賠償が原則である。しかし、金銭賠償だけでは被害者が十分に満足できなかったり、金銭賠償が救済方法として適切でない場合には、損害賠償に代えるか損害賠償と並行して信用回復に必要な措置を求めることができる(営業秘密保護法第12条)。

(2) 法的根拠

第12条(営業秘密保有者の信用回復) 法院は、故意又は過失による営業秘密侵害行為により営業秘密保有者の営業上の信用を失墜させた者には、営業秘密保有者の請求により第11条による損害賠償に代え、又は損害賠償とともに、営業上の信用を回復するために必要な措置を命ずることができる。

(3) 請求要件

営業秘密の侵害を原因とする信用回復請求のためには、①営業秘密侵害行為者の故意又は過失、②営業秘密の侵害行為の存在、③営業秘密保有者の営業上における信用の失墜、④損害賠償以外の別途の信用回復措置の必要性が認められなければならない。

特に、要件④と関連して、権利者の業務上の信用が失墜した点が認められる場合にも、侵害者の侵害行為の態様、侵害行為前後の事情などに鑑みて侵害者に損害賠償を命じることだけで十分に被害者の損害が填補されたと認められる場合には、信用回復請求が棄却されることがある。

(4) 信用回復措置

請求人の信用回復請求が、理由があると法院が判断した場合には、法院は営業秘密の侵害者に対し、営業秘密保有者の営業上の信用を回復するのに必要な措置を取ることを命じなければならない。

例えば、侵害者の侵害罪に対する刑事判決、敗訴した民事判決、釈明資料などを新聞又

は雑誌などに掲載することを命じることができる。ただし、新聞などに謝罪広告を出すように命じることが、憲法上、良心の自由に反するという憲法裁判所の決定により、謝罪広告の請求は不可能である。

3.5 不当利得返還請求権(民法第741条)

(1) 意義及び必要性

営業秘密侵害者の故意又は過失が認められず、損害賠償義務が存在しない場合にも、営業秘密侵害行為によって侵害者は法律上原因なく利益を得ており、これにより営業秘密の保有者が損害を被ることになるが、侵害者が得た利益を営業秘密の保有者に返還すべきである。

損害賠償請求権とは違い、営業秘密保護法において不当利得返還請求権については積極的に規定していない。しかし、営業秘密保護法に規定されていなくても、民法上不当利得返還請求権に関する法理は営業秘密侵害による不当利得の返還請求にもそのまま適用される。

損害賠償請求権と異なる不当利得返還請求権は、故意又は過失のように主観的要件を要さず、損害賠償請求権は3年時効で消滅するのに対し、不当利得返還請求権は消滅時効が10年であるため、損害賠償請求ができない場合には有用な代案となり得る。

(2) 法的根拠(民法)

第741条(不当利得の内容) 法律上、原因なしに他人の財産又は労務によって利益を得て、これによって他人に損害を加えた者は、その利益を返還しなければならない。

(3) 不当利得返還請求要件

(a) 法律上の権原の不在

他人の営業秘密の使用が「法律上、正当な権原なしに」行なわれたものでなければならない。他人の営業秘密を侵害して無断に使用したことがその代表的な例といえる。

ただし、契約などによってその営業秘密を正当に使用する権利を取得した者の営業秘密使用行為に対しては、不当利得返還請求をできないことは明白である。

(b) 営業秘密の侵害者に利益が発生

法律上、権原なしに行なわれた行為によって、営業秘密侵害者に利益が発生しなければならない。利益というのは、その行為がなければ存在する財産総額より、現在ある財産総額が増加した場合には、その増加額にあたる。また、その行為がなかった場合、当然発生した財産上の減少を免れたことによって得る経済的利益も含まれる。

(c) 営業秘密の保有者に損害が発生

他人による法律上権原のない行為によって、営業秘密の保有者に損害が発生しなければならない。不法行為による損害賠償請求とは異なり、該当行為がなければ営業秘密の保有者の財産が増加しただろうと認められる場合にも、損害の発生が認められる。

(d) 営業秘密侵害者の財産上の利益及び営業秘密保有者の損害との間における因果関係の存在

営業秘密侵害者の財産上の利益と営業秘密保有者の損害との間には、相当因果関係が認められなければならない。

(4) 返還利得の範囲

返還する利益の範囲は、被害者が、現実が発生した侵害者の利益と被害者の損害をそれぞれ立証すれば、そのうちの少ない金額が認められることが原則である。不当利得返還請求の場合、損害賠償請求とは異なり返還利益額に関する推定規定を置いていない。

ただし、実務的には侵害者が返還する利益の最低限度として使用料相当額が認められている。

(5) 損害賠償請求権との競合

損害賠償請求権と不当利得返還請求権は同一の事実(営業秘密侵害)を対象とするが、訴訟法的には訴訟物を異にして互いに競合関係にある。したがって、訴訟提起時には損害賠償請求権に基づいたものなのか、不当利得返還請求権に基づいたものなのか明確に特定しなければならず、損害賠償請求権に基づいた訴訟で敗訴し、その判決が確定した場合でも、その後、不当利得返還請求権に基づく請求をすることができる。

3.6 仮処分(民事執行法第300条)

(1) 仮処分訴訟の必要性

前述した営業秘密侵害行為の禁止及び予防請求権(第10条)については、通常、営業秘密保有者の申立てにより、法院が提訴の前後を問わず、本案に関する最終審理以前の段階で、侵害被疑者に暫定的に侵害禁止命令を出す仮処分申請を提起するケースが多い。仮処分が認められると侵害被疑者の生産及び販売が中断されるので、営業秘密保有者には非常に実効的で強力な攻撃手段になり得る。

(2) 要件

仮処分申請が受け入れられるためには、被保全権利が存在し、かつ該当権利の保全の必要性が認められなければならない。

営業秘密侵害禁止の仮処分を請求する場合は、被保全権利は請求人が有する営業秘密保

護法又は産業技術保護法上の侵害禁止請求権である。

また、営業秘密侵害禁止請求権を訴訟を通じて請求して確定判決まで待つ場合は、回復できない損害が発生することが予想される場合などに認められる。したがって、既に債務者の行為でない他の経路によって営業秘密が知らされ、これ以上禁止することがかえって競争を不当に制限する結果になる場合には、保全の必要性は認められない⁵¹。

(3) 仮処分の手続き

請求人が仮処分申請書を作成して管轄法院に提出し、費用を納付すれば、管轄法院において申請書の副本を相手方に渡し、直ちに審問期日が指定される。

一般的には申請書の提出日から2、3週間以内の短期間内に審問期日が開かれることになる。したがって、仮処分請求の相手方としては、対応に十分な時間的余裕を持つことは難しいといえる。

また、技術内容が複雑で、双方が提出した鑑定書上の意見が交錯する場合には、技術説明会の開催や、必要な証人及び鑑定の申請を受けることもある。

審問は通常1～2回で終結することになり、審問が終結した後にも仮処分の決定前までは疎明資料を提出することができる。

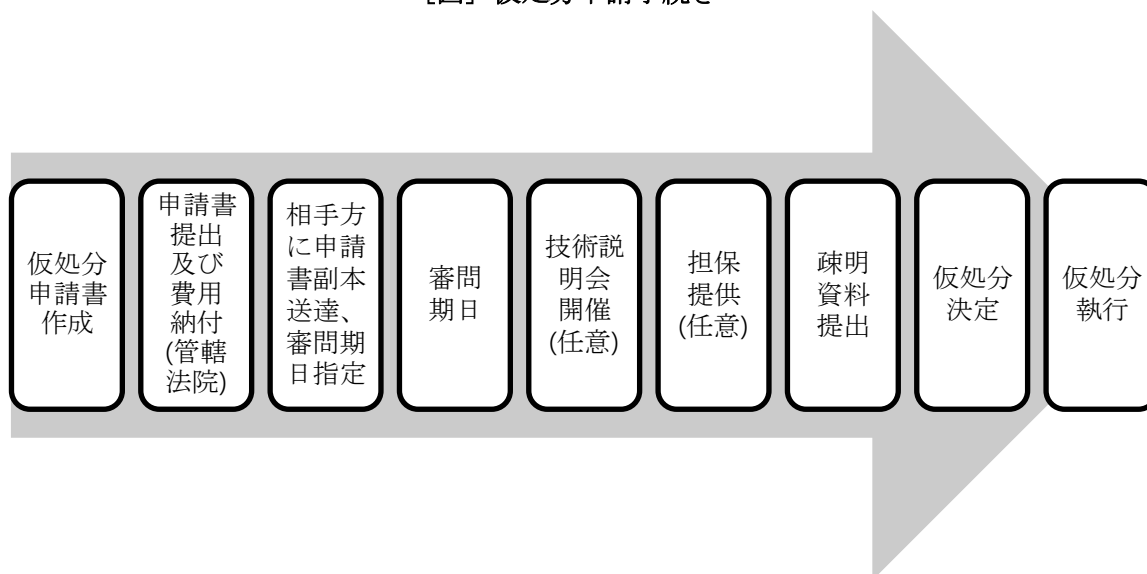
また、法院は仮処分により生じ得る債務者の損害に対し、その後仮処分が誤ったものだと明らかになった場合には、債務者がその損害を容易に回復することができるように、請求人に担保を提供するよう命じることができる。

仮処分決定は、一般的に申請日から3、4ヶ月以内に下され、仮処分を命じる決定は執行力があるため、営業秘密の使用禁止などに対し必要な執行ができる。通常は「侵害禁止義務を履行する時まで、義務違反である1日の所定の金額を支給せよ」という間接強制命令を執行法院から発付される間接強制によって執行される。

仮処分決定を不服とする当事者は、仮処分決定に対する異議申立を行なうことが可能である。

⁵¹ 不正競争防止法(解説及び判例), 司法研修院, 2007, 138面

〔図〕 仮処分申請手続き



(4) 仮処分訴訟の特性

仮処分はあくまでも、本案訴訟に先立ち、臨時的な法律関係の地位を付与することに過ぎず、本案訴訟と同じ終局的な紛争解決の方法でない。したがって、仮処分を申請し、仮処分決定を通じて営業秘密の使用を臨時的に禁止した後には、営業秘密侵害禁止や損害賠償の本案訴訟を提起しなければならない。

したがって、仮処分の効力を維持するためには、請求人が法院から本案提訴命令を受けた日から7日以内に本案訴訟を提起しなければならない。本案訴訟を提起しなければ仮処分決定はその効力を喪失する。

(5) 営業秘密侵害禁止仮処分

本案訴訟を通じて営業秘密侵害禁止請求をする場合、1審裁判の結果が言い渡されるまでだけで10ヶ月以上要するため、判決結果が確定する時点で既に営業秘密侵害禁止期間を徒過してしまい、結局、本案訴訟で敗訴となる可能性が高い。

また、本案訴訟が確定した後には、既にその期間における技術発展によって、該当技術に対する侵害禁止を請求する実益がなくなってしまう場合も多い。

したがって、本案訴訟の結果が出るまで待つ場合は、営業秘密保有者には回復できない損害が生じる恐れがあるため、営業秘密侵害禁止仮処分を請求する必要(保全の必要性)が認められることになる。

(6) 競業(転職)禁止仮処分

営業秘密侵害禁止請求をし、競業又は転職禁止請求をともに請求する場合、1審裁判の結果が言い渡されるまでだけで10ヶ月以上要するため、判決結果が確定する時点で既に前述した競業禁止期間を徒過してしまい、結局、本案訴訟で敗訴する可能性が高い。

したがって、本案訴訟による競業禁止仮処分申請だけでは、権利救済を受け難い急迫した事情が認められる場合には、転職禁止などを目的とする仮処分を申請する必要性(保全の必要性)が認められる。実務的にも競業禁止請求の本案訴訟を提起する際に、仮処分も

ともに申請している。

一方、本案訴訟における競業禁止請求では、禁止期間を定めない場合、懲罰的性格を備えることになり、従業員の職業選択の自由を過度に制限するとして認められないが、競業禁止仮処分の場合、仮処分の特性上、禁止期間を具体的に特定しなかったとして違法であると判断しないのは前述のとおりである。

(7) 誘引採用禁止仮処分

(a) 不当誘引採用の意義

不当誘引採用とは、事業者が取引相手の人材を不当に誘引又は採用して取引相手の事業活動を妨害する行為をいう。これは公正取引法上、禁止される不公正取引行為の類型⁵²に属する。

(b) 該当類型の例示

営業秘密流出と関連して、不当な誘引採用に該当する類型を例示すると次のとおりである。

① 競合他社が営業秘密の流出を目的に、営業秘密を保有する会社に勤務中の職員に個別に接触し、通常の水準に鑑みて過度な待遇措置を取ることを条件として採用する行為

② 競合他社が、他の事業者の技術人材にその会社の重要技術又は製造秘法が記載された書類や設計図などを流出することを条件に、高職位を保障して採用する行為

③ 競合他社が、営業秘密の流出を目的に、他の事業者の核心技術を有する人材に対し、正常な事業の遂行に支障が生じるほど集中的にスカウトをする行為

(c) 民事上の救済方案-誘引採用禁止仮処分など

競合他社の不当誘引採用行為に対しては、該当競合他社に対して採用行為の不作为命令を賦課する仮処分を法院に申請することができる。

また、競合他社の不当誘引採用行為によって損害が生じた場合、民事上の損害賠償を請求することができ、公正取引委員会に不公正取引行為を申告し、又は公正取引紛争調停協議会に紛争調停を申請する方法によって権利救済を受けることができる。

3.7 競業(転職)禁止請求

営業秘密を知っている従業員が退職する場合、競合他社への就職や会社の創業などの過程で、営業秘密が流出する可能性が大きい。したがって、退職者による競合他社への営業秘密の流出を防ぐためには、該当従業員の採用を禁止又は関連業務に従事することを禁止する競業(転職)禁止請求をする必要がある。

競業禁止請求の有効性と禁止期間、起算点などについては、「第4章2. 人的(従業員、退職者など)管理」で既に具体的に説明している。一方、競業禁止義務は不作为義務である

⁵² 公正取引委員会、不公正取引行為の類型及び基準告示、第8条

ため、本案訴訟又は仮処分の決定を通じて競業禁止請求が受け入れられる場合でも、これを直接的に強制することは難しい。

したがって、本案訴訟での確定判決や仮処分決定により、従業員が従業員などに転職禁止などを命じる命令を下し、これを違反した場合には上記の確定判決を執行権として「義務を履行する時まで、義務違反である1日当たりの所定の金額を支給せよ」という間接強制命令を執行法院から発付され、義務の履行を間接的に強制することができる。

3.8 間接強制

営業秘密侵害禁止及び予防義務は不作為義務であるため、本案訴訟又は仮処分決定を通じて営業秘密侵害禁止請求が受け入れられる場合にも、これを直接的に強制することは難しい。

したがって、本案訴訟での確定判決や仮処分決定を通じて営業秘密侵害禁止を命じる命令をしても、これを違反した場合には上記の確定判決を執行権とし、「義務を履行する時まで、義務違反である1日当りの所定の金額を支給せよ」という間接強制命令を執行法院から発付され、義務の履行を間接的に強制することができる。上記のように、判決が確定した後、執行手続きにおいて執行法院を通じて間接強制を実現する方法が一般的だが、判例によれば、『判決が確定するにしても短期間内に債務者がこれを違反する可能性があって、その判決手続きで適切な賠償額を算定できる特殊な場合』には、該当判決手続きにおいて将来その債務者が債務を不履行した場合に一定の賠償をすることを命じることができる。

したがって、必要によっては、営業秘密侵害禁止を請求するとき、間接強制と関連して請求をとにもすることを考慮できる。

3.9 侵害禁止・予防請求権の時効

営業秘密保護法第14条によれば、営業秘密請求権は①営業秘密の保有者がその侵害行為によって営業上の利益が侵害され、又は侵害される恐れがあるという事実及び侵害行為者を知った日から3年間行使しなければ時効によって消滅すると規定している。また、同条によれば、②その侵害行為が始まった日から10年が経過した場合でも時効によって消滅すると規定している。上記二つの期間中、いずれか一つの期間でも経過する場合には侵害禁止・予防請求権は時効によって消滅する。

したがって、営業秘密侵害に対する侵害禁止・予防請求権の時効が進行するためには、少なくとも営業秘密の侵害行為が実際に開始されなければならない、さらにその侵害行為によって自らの営業上の利益が侵害され、又は侵害される恐れがある事実及び侵害行為者を知っておかなければならない。

大法院の判例でも、上記のような法理を適用して、被告が、原告が生産しているスピンパックフィルターと類似のフィルターを生産・販売するために会社を設立したとしても、そのように会社を設立した時点で直ぐに侵害行為が開始されたと見なすことはできないとし、また被告の会社が設立された時点から消滅時効が進行されたと見なすことはできないと判断した。

3.10 民事的解決方法の限界

(1) 証拠収集の難しさ

営業秘密侵害事件の場合、証拠が大部分侵害者の手元にある場合が多く、米国のような証拠開示制度を導入していない韓国の場合、侵害者が所有している証拠を確保するには限界がある。したがって、民事上の救済手続き内では、営業秘密の侵害行為を立証するための証拠を確保することが容易でないため、敗訴するが多い。

(2) 営業秘密立証の難しさ

営業秘密保護法に基づく民事上の救済措置を利用するためには、流出した情報が営業秘密保護法上の営業秘密の成立要件を満たすものでなければならない。しかし、営業秘密の成立要件が過度に厳格であり、特に、秘密保持性に関して、該当情報が秘密として保持された事実を客観的に立証することは容易ではないため、実務的には該当情報が営業秘密と認められないことを理由に敗訴となるケースが多い。

(3) 損害額立証の難しさ

営業秘密侵害と相当の因果関係のある損害額を特定することは容易ではなく、このため、営業秘密保護法では第14条の2で損害額推定規定を設けているが、上記推定規定の適用を受けるのに必要な資料は相当な部分が侵害者の手元にある。

この問題を解決するために、営業秘密保護法第14条の3では、資料提出義務を規定しているが、この場合も、資料提出を拒否する正当な理由がある場合には提出を拒否でき、実務的には資料提出拒否の理由が幅広く認められており、上記の規定の趣旨が失われている。

(4) 侵害禁止請求の実益

営業秘密侵害禁止請求の場合、営業秘密を侵害した会社が国内で製品を生産する場合には実益があるが、国内に支社がない国外企業により営業秘密が侵害される場合には、損害賠償を請求するほか、営業秘密の侵害禁止などを請求する実益が大きい。

4. 刑事的解決方法

近年、営業秘密侵害事件の発生時に、対応手段として刑事告訴、告発を選択するケースが増えている。特に、刑事告発の場合、①訴訟費用がかからず、②捜索・押収などを通じて証拠確保が容易であるため、多くの被害企業が刑事救済手続きを利用する頻度が増えている。

営業秘密侵害事件の発生時、損害賠償請求、侵害禁止仮処分などを申請するためには、関連事件に対する証拠の確保が切実だ。しかし、韓国では、米国のような証拠開示制度を採択していないため、被害企業が、加害者が保有していると推定される証拠を確保することは容易ではない。

したがって、営業秘密侵害禁止仮処分や損害賠償請求のような民事上の救済手続きを履

行する前に、加害者の証拠隠滅を防止し、加害者が保有している証拠を確保するために、刑事告訴とともに迅速に捜索・押収を要請することが先制的手段として活用されているのが実情である。

4.1 営業秘密保護法による対応

営業秘密侵害行為に関しては、基本的に営業秘密保護法上の営業秘密侵害罪が問題となる。営業秘密保護法が適用されるためには、流出した情報が、営業秘密保護法上の営業秘密成立要件を満たすことを前提とする。

また、侵害時には、両罰規定により、侵害者個人だけでなく、所属する組織及び企業も処罰を受けることになり、侵害の予備、陰謀の場合でも処罰の対象となる。

4.2 特別法による対応

流出した営業秘密が技術情報に関する場合には、産業技術保護法第4条に基づく特別法優先の原則に従い、営業秘密保護法等の適用に先立って産業技術保護法が適用されることになる。産業技術保護法が適用されるためには、流出した情報が産業技術保護法上の産業技術又は国家コア技術に該当するものでなければならない。また、流出した営業秘密が防衛産業技術に該当する場合、防衛産業技術保護法違反による刑事的措置をとることができる。

また、営業秘密流出の経緯が、当該営業秘密保有企業の情報通信網を侵害して行われた場合には、情報通信網侵害罪が成立できる。

(1) 産業秘密保護法による刑事上の救済の長所及び短所

(a) 長所

① 処罰量刑の強化

営業秘密保護法と比べて法規定上の罰金の金額が高額であり、実際に判決を下される懲役量刑も営業秘密保護法に比べて多い。即ち、産業技術保護法による刑事上の救済時には、営業秘密保護法による場合よりも重刑に処する可能性が高いため、その後訴訟上の和解などを行う時は有利な位置を占めることができる。

② 立証の責任の緩和

産業秘密保護法では、第36条による刑事上の処罰規定における「不正な利益を得る目的又は産業技術保有者に対して損害を加える目的」のような不正な目的を要求していないため(第14条第2号による処罰規定除外)、構成要件に関する立証責任が営業秘密保護法と比べ緩和されている。

(b) 短所

① 産業技術の概念の曖昧性

産業技術の範囲が、個別法令にしたがって関係中央行政機関長によって指定されるため、

指定の主体及びその根拠法令が多様で、これを一つ一つ確認するのは困難である。したがって、検察では「産業技術」であるかどうかを判断するよりは、法定刑と保護対象が類似する営業秘密保護法を主に適用しており、産業秘密保護法の適用事例が徐々に減っているのが実情である。

② 必要的没収規定の実効性

産業技術保護法では第36条第4項の規定により、産業技術流出犯罪を犯した者がその行為によって得た財産は没収し、これを没収できない場合には、その財産相当額を追徴するようにしている。

したがって、産業技術を不正に取得したが、これを直接使用又は外部に流出せず、いかなる具体的な経済的利益を得なかった場合には、該当侵害製品を押収・没収するのが困難であるだけでなく、その価額を算定して推定し追徴するのは容易でないという指摘がされている。

4.3 一般刑法及び商法による対応

営業秘密保護法上の営業秘密又は産業技術保護法上の産業技術に該当しない場合でも、刑法において規定する違法行為の要件を満たす場合は、当該規定に基づいて処罰が可能である。

企業内部者による営業秘密侵害行為に関しては、刑法上、業務上秘密漏洩罪(第317条)、横領罪(第355条第1項)、業務上横領罪(第35条)、背任罪(第355条第2項)、業務上背任罪(第356条)などが成立する可能性がある。

そして、企業外部者の営業秘密侵害に関しては、秘密侵害罪(第316条)、窃盗罪(第329条)が成立する可能性がある。

そして、会社の発起人、取締役、監査など会社の営業に関するある種類又は特定事項の委任を受けた使用人が、その任務に違反した行為で営業秘密を流出した場合、商法上特別背任罪(商法第622条第1項)が適用できる。また、上記行為によって得た財産上の利得額が50億ウォン以上の場合、特定経済犯罪加重処罰法による加重処罰(特経法第3条)を受けることがある。

[表21]

適用法律		禁止行為	処罰量刑	予備・陰謀行為の処罰	未遂犯の処罰
刑法	業務上背任	単純背任行為	5年以下の懲役 1500万ウォン以下の罰金	×	○
		業務上背任行為	10年以下の懲役 3千万ウォン以下の罰金		
	窃盗罪	情報が収録された物品の無断窃盗行為	6年以下の懲役 1千万ウォン以下の罰金	×	○

	財物 損壊罪	文書、電子記録媒体 などを損壊・隠匿 する行為	3年以下の懲役 700万ウォン以下 の罰金	×	○
	秘密 侵害罪	封書、秘密装置など の無断開封行為	3年以下の懲役 500万ウォン以下 の罰金	×	×
	業務 妨害罪	他人の業務妨害 情報処理装置などの 破損	5年以下の懲役 1500万ウォン以下 の罰金	×	×

4.4 公訴事実に対する立証責任

民事訴訟とは違い、刑事裁判では、公訴が提起された犯罪事実に対する立証責任は検察官にある。また、民事訴訟とは違い公訴事実に対する立証の程度は、裁判官にとって合理的な疑いを持つ余地がないほど公訴事実が真実だという確信を持てるような強力な証明を要する。

一般的に、刑事事件の被疑者は有罪の確定判決を受ける前までは無罪と推定される権利を有する。何人も疑いだけでは処罰を受けない権利があり、合理的な疑いが排除されるほど確実な証拠が無ければ有罪の判決を受けない権利がある。

したがって、犯罪事実に対する疑いを生じさせる証拠だけでは不十分であり、裁判官に犯罪事実の存在を確信させることができる強力な証拠が存在しない場合には敗訴の可能性が高い。

＜裁判官に犯罪事実を確信できる証拠が提出されない事件において営業秘密違反罪が不認定とされた判例＞

－昌原地方法院 2009. 2. 12. 宣告 2008ノ599 判決

『本件ファイルが相当な努力によって営業秘密として保持・管理されたという点に対し、合理的な疑いの余地なくこれを認めるのは難しく、検察官が提出した各証拠だけではこれを認めるに足りない。したがって、被告人に営業秘密違反罪を認めることはできない。』

4.5 営業秘密侵害が共同で行なわれた場合の扱い

営業秘密侵害行為には直接加担しなかったが、共謀行為にだけ加担した場合でも共同正犯に該当することになる。したがって、2人以上で共謀して営業秘密侵害が行なわれた場合、共謀者が営業秘密侵害行為に直接加担したか否か、また秘密保持義務が存在するか否かに関係なく、共謀行為の成立だけでも営業秘密侵害罪の共同正犯によって処罰されることになる。

4.6 未遂犯などに対する扱い

未遂とは、犯罪の実行に着手したが行為を終了できなかったり、終了したとしても結果

が生じない場合をいう。未遂は、実行に着手したという点から、後述する予備・陰謀行為とは区別される。

営業秘密保護法では、同法第18条第1項及び第2項の営業秘密侵害行為の未遂犯も処罰されるようにしており、刑法第25条によれば、未遂犯の場合、既遂犯よりも減刑できるようにしている。

一方、営業秘密侵害行為に至るための各行動段階において、どの時点で着手が成り立ち、どの時点から既遂なのかどうか争点となる。これと関連して大法院の判決では、営業秘密不正使用罪の実行の着手時期について「営業秘密不正使用罪においては、行為者が当該営業秘密と関係した営業活動に利用あるいは活用する意思の下、その営業活動にアクセスした時期に営業秘密を閲覧する行為(営業秘密が電子ファイルの形態である場合には、保存の段階を越えて該当電子ファイルを実行する行為)をしたならば、その実行の着手がある」と判示している⁵³。

一方、上記大法院の判決の原審判決であるソウル高等法院での判決⁵⁴では、営業秘密の使用による営業秘密保護法違反罪の既遂と未遂を次のとおり区分している。

[表22] 営業秘密保護法違反罪の既遂・未遂の区分

段階	行為の態様	区分
0	取得	-
1	保存又は備置	実行の着手なし
2	閲覧	未遂
2-1	閲覧後の利用性・活用性 考慮中	未遂
3	実行(利用又は活用)	既遂
4	結果(未完成を含む)	既遂

4.7 予備・陰謀行為に対する扱い

予備は犯罪意思の実現のための準備行為をいい、陰謀とは、2人以上が一定の犯罪を実現するために互いに意思を交換する行為をいう。

予備と陰謀は、まだ実行の着手には至らなかったが、実行の着手に時間的・場所的に密接に関連した準備行為をいう。

営業秘密保護法では、第18条の3で第18条第1項及び第2項の罪を犯す目的で予備又は陰謀をした者を次のとおり懲役刑又は罰金刑に処するようにしている。この場合、第18条第1項及び第2項で規定している主観的要件が満たされることを前提とする。

[表23] 営業秘密侵害行為を予備・陰謀した者に対する罰則

営業秘密侵害行為	予備・陰謀時の罰則規定

⁵³ 大法院 2009. 10. 15. 宣告 2008ト9433 判決

⁵⁴ ソウル高等法院 2008. 10. 2. 宣告 2008ノ1289 判決

不正な利益を得たり、営業秘密の保有者に損害を加える目的で、その営業秘密を外国で使用又は外国で使用されると知りながら取得・使用又は第三者に漏えい(営業秘密保護法第18条第1項)	3年以下の懲役又は3千万ウォン以下の罰金 (営業秘密保護法第18条の3第1項)
不正な利益を得たり、営業秘密の保有者に損害を加える目的で、その営業秘密を取得・使用又は第三者に漏えい(営業秘密保護法第18条第2項)	2年以下の懲役又は2千万ウォン以下の罰金 (営業秘密保護法第18条の3第1項)

4.8 刑事的解決方法の限界

(1) 低い処罰水準

近年の営業秘密侵害刑事事件をみると、ほとんどで執行猶予外罰金刑が下され、懲役刑の実刑が言い渡されたケースがほとんどなく、処罰水準が低いことが分かった。こうした低い処罰水準により、加害企業や職員は自身の犯罪行為に対して特に罪意識を持たなくなり、被害者は刑事告訴や告発などの措置を積極的に取ることに躊躇するようになるという問題点がある。

(2) 立証の困難性

営業秘密は、企業が保有する高度な技術的知識をその内容としているため、法の執行のためには、法院及び検察の両方が当該技術について深く理解することが前提とされるべきだが、実務を担当している判事や検事などは当該技術に門外漢である場合が多く、当該営業秘密の技術的価値に対する評価などが困難な場合が多い。

(3) 訴訟過程における営業秘密の追加流出の懸念

民事訴訟と同様に刑事訴訟も公開裁判で行われるため、訴訟進行中に営業秘密が外部に公開されるおそれがある。

5. その他の紛争解決方法

5.1 公正取引委員会への申告

大企業が不当に技術資料の提供を要求するか、又は書面化された合意に違反して要求を受けた技術資料を流用するなど、下請法第12条の3の規定に違反して下請関係にある中小企業が保有する営業秘密を侵害した場合、公正取引委員会に申告することができる。申告の内容が不公正取引行為に該当する場合には、当該大企業に対して是正措置、課徴金、罰金賦課又は損害賠償などの罰則が与えられることになる。

5.2 貿易調査委員会への調査依頼

営業秘密を侵害した物品等を国内で製造、又は販売する行為等については、「不正貿易行為調査及び産業被害救済に係る法律」に基づき、貿易委員会の貿易調査室に調査要請をすることができる。貿易委員会により調査開始の決定が行われ、事件の調査が行われた結果、不正貿易行為に該当すると判定されたときは、貿易委員会は、是正措置(法第10条)、課徴金(法第11条)を科すことができ、課徴金義務者が納付期限内に課徴金を納付しない場合、履行強制金を徴収(法第13条の2)する。

[表24] 不正貿易行為調査対象項目

区分	調査対象項目
知的財産権侵害 ⁵⁵	-知的財産権(特許権、実用新案権、デザイン権、商標権、著作権、著作隣接権、プログラム著作権、半導体集積回路の配置設計権、地理的表示、営業秘密)を侵害する物品などを国内で販売し、又は輸出目的で国内で製造する行為
原産地表示違反 ⁵⁶	-原産地を虚偽に表示又は誤認させる表示をした物品などを輸入あるいは輸出する行為 -原産地表示を損傷又は変更した物品などを輸入あるいは輸出する行為 -原産地表示をしていない原産地表示対象物品などを輸入あるいは輸出する行為
輸出入秩序阻害 ⁵⁷	-品質などを虚偽に表示又は誇張して表示した物品等を輸入あるいは輸出する行為 -輸出又は輸入物品等の引渡・買収、代金の決済など輸出入の契約事項を契約内容どおりに履行せず、対外信用を損傷させ、当該地域に対する輸出あるいは輸入に支障を与える行為 -契約内容と顕著に異なる物品などを輸出又は輸入、あるいは輸出又は輸入と関連し、紛争などを故意に起こすことにより、対外信用を損傷させる行為

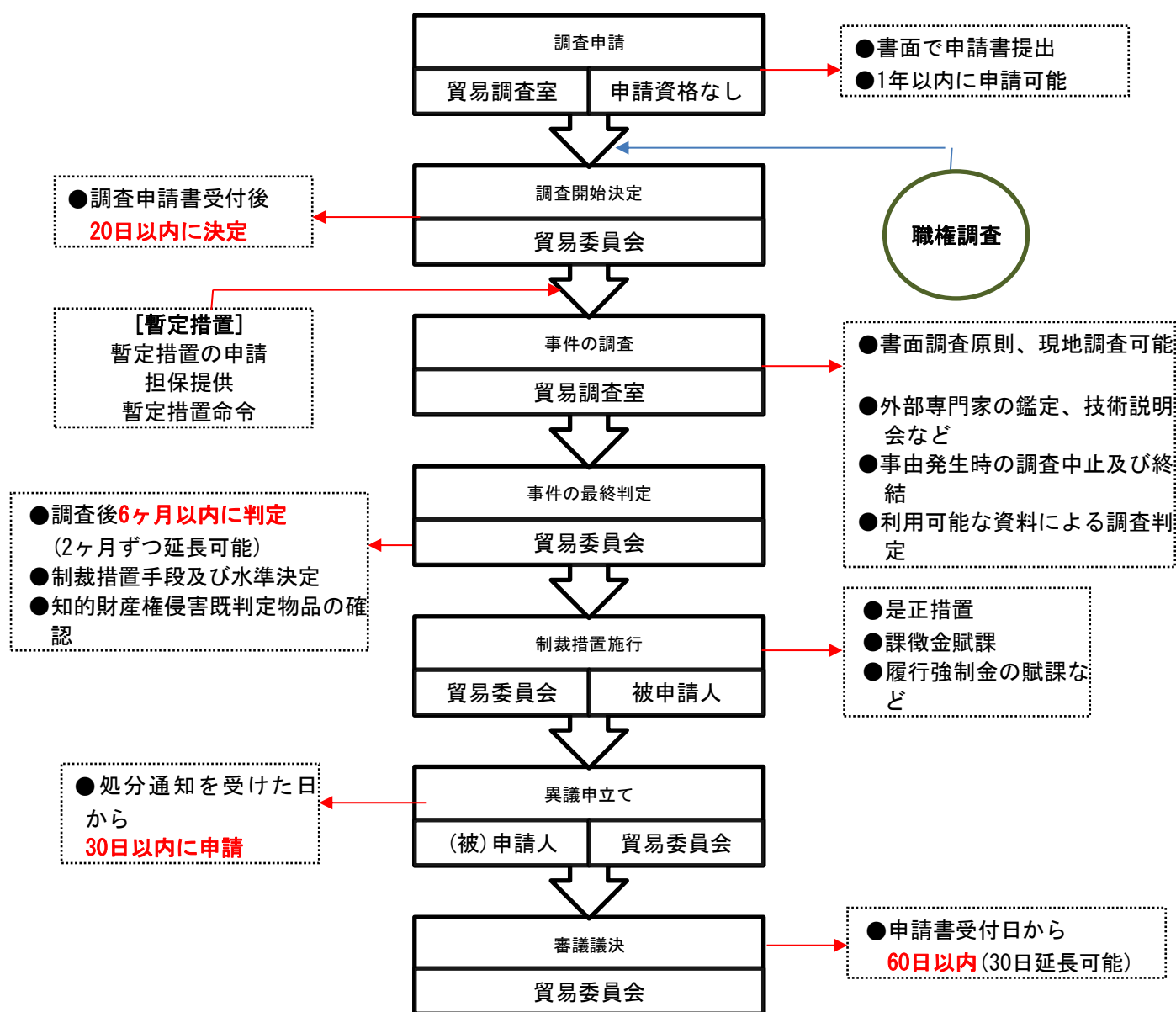
出典：貿易委員会(<http://www.ktc.go.kr>)

⁵⁵ 不正貿易行為調査及び産業被害救済に関する法律第4条第1号違反

⁵⁶ 不正貿易行為調査及び産業被害救済に関する法律第4条第2号違反

⁵⁷ 不正貿易行為調査及び産業被害救済に関する法律第4条第3号違反

[図] 不公正貿易行為の調査手順



このように、営業秘密を侵害した物品などを国内で製造又は販売する行為などに対しては、貿易委員会の貿易調査室に調査要請をすることができる。貿易委員会によって調査開始の決定がなされ、事件の調査が行なわれた結果、不公正貿易行為に該当すると判定された場合には、貿易委員会は次のとおり、是正措置や課徴金を賦課することができ、課徴金の納付義務者が納付期限内に課徴金を納付しない場合には、加算金を徴収することができる。

[表25] 不公正貿易行為時の罰則

不公正貿易行為時の 罰則	不公正貿易行為調査及び産業被害救済に関する法律の内容
是正措置	当該侵害物品などの輸出又は輸入販売製造行為の中止、当該物品などの搬入の排除及び廃棄処分、訂正公告、貿易委員会から是正命令を受けた事実の公表及びその他是正のための必要な措置を命令(第10条)
課徴金賦課	大統領令が定める取引金額に100分の30をかけた金額を超過しない範囲内で課徴金賦課、ただし、取引金額がない場合、又は取引金額の算定が困難な場合として、大統領令が定める場合には5億ウォンを超過しない範囲で課徴金賦課(第11条)
履行強制金賦課	課徴金の納付義務者が納付期限内に課徴金を納付しない場合には、納付期限の翌日から納付する日までの期間に対し、課徴金金額の100分の5の範囲内で大統領令が定める加算金を徴収(第13条)

5.3 調停及び仲裁

(1) 意義

調停は、訴訟によらず、中立的な位置にある第三者の勧告によって紛争当事者間の合意を図る手続である。そして、仲裁とは、当事者間の合意(仲裁合意)により、当事者間の紛争を法院の訴訟手続によらず、第三者を仲裁人に選定し、その紛争の解決を仲裁人の決定に委ねるとともに、最終的にその決定に従うことで紛争を解決する手続をいう。

調停及び仲裁の内容は確定判決と同一の効力を有し、したがって、不応時には強制執行の行使が可能である。

(2) 調停、仲裁機関

韓国特許庁は2020年改正発明振興法の施行により、2020年8月5日から、営業秘密保護法に定められた不正競争行為及び営業秘密全般に関する紛争についても、産業財産権紛争調停委員会⁵⁸において調停が可能とした。

また、仲裁法に基づく仲裁機関としては、大韓商事仲裁院、ソウル地方弁護士会、韓国著作権委員会などがある。

(3) 長所と短所

⁵⁸ https://www.koipa.re.kr/adr/request_2.html (産業財産権紛争調停委員会オンライン申請ホームページ)によるオンライン受付、又はホームページからダウンロードした様式を利用して郵便、ファックス又は電子メールで申請書提出が可能。

調停や仲裁による場合、訴訟より迅速に結論を導き出すことができ、特に産業財産権紛争調停委員会を介する場合、調停費用が無料で、すべての手続きが非公開で進められるという点において、訴訟より有利な面がある。

ただし、調停の場合、訴訟と違って、国家権力による強制性がないため、調停案を受諾するかどうかは当事者の自由意思にかかっている。したがって、ある当事者の一方が調停に応じないと、紛争解決が遠のくという短所がある。

なお、仲裁の場合、法律に拘束されて判断する訴訟と異なり、仲裁人の主観が介入するおそれがある。また、不服申立ての手段がないため、両当事者の主張を形式的に折衝する線で終わる場合が多い。

第 3 編 各種関連書類参考書式(フォーム)

前述したように、営業秘密保護体制を構築するためには秘密保持契約書、営業秘密管理規定など様々な書式の書類を作成する必要がある。このため、特許庁、国家情報院、中小企業庁などの公共機関及び民間機関では、各種営業秘密保護関連書式を提供している。

以下本編では、特許庁の営業秘密保護センターで公開している標準書式に基づいて、関連書類の参考書式を開示している。このような標準書式はそのまま使用してはならず、各企業の規模、業種、及び営業秘密の特性などによって適切に修正又は変更して活用しなければならない。

1. 内部関係用標準書式

1.1 入社者との秘密保持契約書の例

秘密保持誓約書(入社者)

所属：

氏名：

生年月日： ____年__月__日

私は、20__年__月__日付で株式会社ABC(以下「会社」という。)に入社し、会社から営業秘密及び営業資産の重要性と営業秘密等の保護に係る法令及び会社の就業規則、営業秘密管理規定その他の社規、方針、政策等に関して十分な説明を受け、その内容を理解した上で、以下の事項を遵守することを誓約します。

1. 私は、以下の情報が会社の営業秘密に該当することを確認し、会社の就業規則、営業秘密管理規程その他の社規、方針、政策等を遵守することを誓約します。
 - ① 営業秘密管理規定その他会社の内部規定に記載された営業秘密保護対象
 - ② 営業秘密が表示された技術資料、工場配置図、製品設計図、金型、試作品、製造及び販売マニュアル、製造原価、販売及び価格決定、取引先資料、人材情報などに関する情報など
 - ③ 統制区域、施錠装置、パスワードなどでアクセスが制限されたコンピュータシステム、保管ロッカー、統制区域に保管されている記録媒体、文書、物、情報など
 - ④ [追加事項記載]
 - ⑤ その他会社が営業秘密として指定・表示、又は会社が営業秘密として管理している秘密情報
2. 私は、会社に在職中に取得することになる会社の営業秘密、会社の研究開発・営業・財産などに影響を及ぼしうる有形・無形の情報その他会社の主要営業資産を在職時はもちろん、退職後にもこれを秘密に保持し、会社の事前書面同意なしには競合他社や第三者に提供又は漏洩せず、不正な目的で公開又は使用しないことを誓約します。
3. 私は、会社に在職中に取得することになる会社の営業秘密、会社の研究開発・営業・財産などに影響を及ぼしうる有形・無形の情報その他会社の主要営業資産に対するすべての権利が会社の所有であることを認め、これを会社に帰属させることを誓約します。

4. 私は、会社に在職中に、会社の承認を受けなければ、統制区域、許可を受けていない情報、施設等にアクセスせず、会社の営業秘密を複製、又は写し等の形態で保管しないことを誓約します。
5. 私は、入社前又は在職中に取得した他人の営業秘密等に該当する情報を会社に提供又は開示せず、業務上その情報の開示が避けられないと判断する場合には、事前に会社と相談し、他人の営業秘密等を侵害しないことを誓約します。
6. 私は、会社に在職中に、会社の事前承認を受けない限り、会社と同種、類似業種の企業の役職員として兼職しない、又は諮問をしないことを誓約します。
7. 私は、会社のコンピュータ等の情報処理装置及び情報通信ネットワークを業務用에만使用し、会社が不法行為防止及び営業秘密等の保護のために必要な場合、私のコンピュータ等の情報処理装置や電子メール又はインターネット等の情報通信ネットワークの使用内訳、その他必要な情報をモニタリングすることができ、違法行為又は営業秘密等の漏洩や侵害の恐れがある場合、関連内容を閲覧することを理解し、これに同意します。
8. 私は、退職時に、在職中に保有していた会社の営業秘密、会社の研究開発・営業・財産等に影響を及ぼしうる有形・無形の情報、その他会社の主要営業資産に関する資料の全てを会社に返却し、これに関するいかなる形の写しも個人的に保有せず、返却できないものは廃棄することを誓約します。

上記の誓約事項に違反した場合、関連法規による民事・刑事上の責任を負うことを誓約します。

（上記の内容を確認して理解し、これに署名する）

20__ . __ . __.

誓約者： （署名）

株式会社ABC御中

1.2 在職者との秘密保持契約書の例

秘密保持誓約書(在職者)

所属：

氏名：

生年月日： ____年 ____月 ____日

私は、株式会社ABC(以下「会社」という。)に[]年[]月[]日に入社し、現在在職中の役職員であり、会社から営業秘密及び営業資産の重要性と営業秘密等の保護に係る法令及び会社の就業規則、営業秘密管理規程その他の社規、方針、政策等に関して十分な説明を受け、その内容を理解した上で、下記の事項を遵守することを誓約します。

1. 私は、在職中に業務遂行の過程で取得した会社の営業秘密、会社の研究開発・営業・財産等に影響を及ぼしうる有形・無形の情報、その他会社の主要営業資産を秘密に保持し、これに関する法規及び会社の就業規則、営業秘密管理規定その他の社規、方針、政策等を遵守いたします。
2. 私は、在職中に「営業秘密に関する業務記載」に関する業務を遂行する過程で取得した下記のような情報等が、会社の営業秘密あるいは主要営業資産であることを明確に認識しています。

区分	営業秘密/営業資産の名称	営業秘密/営業資産の説明
1		
2		
3		
4		

3. 私は、業務の遂行中又は業務と関係なく取得することになる会社の営業秘密、会社の研究開発・営業・財産等に影響を及ぼしうる有形・無形の情報、その他会社の営業上の主要資産を、指定された業務に使用する場合を除き、会社の書面による事前の同意なく、いかなる方法であっても競合他社や第三者に提供又は漏洩せず、不正な目的で公開又は使用しないことを誓約します。
4. 私は、在職中に取得した会社の営業秘密、会社の研究開発・営業・財産等に影響を及ぼしうる有形・無形の情報、その他会社の主要営業資産に関するすべての権利を会社に帰属させることを誓約します。

- 私は、会社に在職中に、会社の承認を受けない限り、統制区域、許可を受けていない情報、施設等にアクセスせず、会社の営業秘密を複製又はコピー等の形で保管しないことを誓約します。
- 私は、会社に在職中に、会社の事前承認を受けない限り、会社と同種、類似業種の企業の役職員として兼職又は諮問を提供しないことを誓約します。
- 私は、退職時に、会社に在職中に保有していた会社の営業秘密、会社の研究開発・営業・財産等に影響を及ぼしうる有形・無形の情報、その他会社の主要営業資産及びそれに関する資料のすべてを会社に返却し、それに関するいかなる形の写しも個人的に保有せず、返却できないものは廃棄することを誓約します。
- 私は、退職時には、退職日から[]年の期間、会社と合意した地域及び職務について会社の営業秘密あるいは営業資産が漏洩又は利用される可能性のある企業、団体に就職、又はそのような企業や団体を創業、又は設立して競争しないことを誓約します。もし、私が就業又は創業しようとする企業又は団体が本誓約書による競業禁止の対象となるか、対象であるかどうかが不明な場合、事前に会社に通報し、会社の確認及び同意を得ることを誓約します。

上記の誓約事項に違反した場合、関連法規による民事・刑事上の責任を負うことを誓約します。

(上記の内容を確認して理解し、これに署名する)

20____. _____. _____

誓約者: (署名)

株式会社ABC御中

1.3 退職後の競業禁止契約書の例

秘密保持誓約書(退職者)

所属:

氏名:

生年月日: ____年__月__日

私は[]年[]月[]日付で株式会社ABC(以下「会社」という。)を退職するにあたり、会社の営業秘密及び営業資産の保護のため、以下のとおり誓約します。

1. 私は、[]年[]月[]日付で会社に入社し、最終的に以下のような業務を遂行しました。

[部署名/職責/役職] _____

[業務内容] _____

2. 私は、会社に在職中に取得した下記のような営業秘密及び営業資産を含め、その他会社の営業秘密及び営業資産が会社の所有であることを明確に認識しており、退職後もこれを秘密に保持することはもちろん、会社の事前書面の同意なしに競合他社又は第三者に提供したり漏洩したりせず、不正な目的で使しないことを誓約します。

区分	営業秘密/営業資産の名称	営業秘密/営業資産の説明
1		
2		
3		
4		

3. 私は、会社を退職した日から[]年間、下表に定める地域内で下表に定める業務に関し、上記第2項の営業秘密及び営業資産を含め、その他会社の営業秘密及び営業資産が漏洩、又は利用される可能性のある企業又は団体に就業、又はそのような企業又は団体を創業又は設立して会社と競争しないことを誓約します。もし、私が就業又は創業しようとする企業又は団体が本誓約書による競業禁止の対象となるか、対象であるかどうか不明な場合、事前に会社に通報し、会社の確認及び同意を得ることを誓約します。

[競業禁止地域] _____

〔競業禁止業務〕 _____

4. 私は、退職時に会社から金[]ウォンを上記の秘密保持及び競業禁止約定の対価として別途支払いを受け、また退職後[]年になる時点及び[]年になる時点において、本誓約書に基づく義務遵守事実を会社に通知し、事実と確認された場合、各金[]ウォンの支払いを受けることに約定しました。
5. 私は、第2項及び第3項に定める義務に違反した場合、それによる損害賠償として金[]ウォンを会社に支払い、これとは別に上記第4項により支払いを受けた金銭及びこれに対する支払日からこれを返還する日までの法定利息を追加して、会社に返還することを約束します。
6. 私は、退職時に、第2項の営業秘密及び営業資産を含め、その他会社の営業秘密及び営業資産に関する資料を添付の営業秘密資料返却確認書と共に返却し、返却できないものは廃棄し、これに関するいかなる形の写しも個人的に保有しないことを誓約します。
7. 私は、退職後、私が在職中に使用したコンピュータ等情報処理装置や電子メール又はインターネット等の情報通信ネットワークの使用内訳、その他必要な情報を会社が調査することができ、不法行為又は営業秘密等の漏洩や侵害の恐れがあるときには、関連内容を閲覧することができることを(理解し、これに同意します。)

添付： 営業秘密資料返却確認書⁵⁹ 1部(○ページに様式掲載)

(上記の内容を確認して理解し、これに署名する)

20__ . __ . __

誓約者： (署名)

株式会社ABC御中

⁵⁹ 本編115ページに様式掲載

1.4 訪問者との秘密保持契約書の例

（秘密保持誓約書（統制区域立入者））

所属：

氏名：

生年月日： ____年 ____月 ____日

私は株式会社ABC（以下「会社」という。）の保護統制区域に立入るにあたり、会社の営業秘密及び営業資産の重要性と営業秘密等の保護に係る法令及び会社の営業秘密管理規定、その他の社規、方針、政策等に関して十分な説明を受け、その内容を理解した上で、以下の事項を遵守することを誓約します。

1. 私は、会社の保護統制区域である[] 統制区域/場所を記載
[]に立ち入るにあたり、会社が秘密情報であることを表示するか、又は口頭で秘密情報であることを説明しながら公開した一切の情報（以下「営業秘密」という。）を秘密に保持し、会社の事前の書面同意又はこれに代えうる関連契約がある場合を除いては、私が所属している企業や団体その他第三者に提供又は漏洩せず、不正な目的で公開又は使用しないことを誓約します。
2. 私は、会社が定めた[]年[]月[]日から[]年[]月[]日まで上記保護統制区域に立入りし、その期間が満了した以降はいかなる事由であっても上記保護統制区域に立入りせず、必要な場合は再び会社から上記保護統制区域に対する立入許可を受けることを誓約します。

私が上記の誓約事項に違反した場合、関連法規及び契約による民事・刑事上の責任を負うことを誓約します。

（上記の内容を確認して理解し、これに署名する）

20__ . __ . __

誓約者： （署名）

株式会社ABC御中

1.5 協力会社との秘密保持契約書の例

秘密保持誓約書(協力会社)

株式会社XYZ(以下「XYZ」という)は、株式会社ABC(以下「ABC」という)と相互協力関係を維持するにあたり、ABCの営業秘密及び営業資産の重要性と営業秘密等の保護に係る法令及びABCの営業秘密管理規程その他の社規、方針、政策等に関して十分な説明を受け、その内容を理解した上で、以下の事項を遵守することを誓約します。

1. XYZは、ABCとの(協力関係に基づく契約名称等)契約(以下「協力契約」という。)を履行する過程で取得することになるABCの営業秘密、ABCの研究開発・営業・財産等に影響を及ぼしうる有形・無形の情報、その他会社の主要営業資産を秘密に保持し、これに関する法規、契約及びABCの営業秘密管理規定、その他の社規、方針、政策等を遵守することを誓約します。
2. XYZは、契約を履行する過程で取得することになるABCの営業秘密、会社の研究開発・営業・財産等に影響を及ぼしうる有形・無形の情報、その他ABCの主要営業資産を、指定された業務に使用する場合を除き、ABCの事前の書面同意なしには、いかなる方法であっても第三者はもちろん、ABCの役職員にも提供又は漏洩せず、不正な目的で公開又は使用しないことを誓約します。
3. XYZは、ABCから事前に許可されていない統制区域又は情報、施設などにはアクセスせず、ABCから便宜上提供されたシステムID、パスワード、出入証等はXYZのみが使用し、他人に公開・貸与・譲渡せず、契約終了時にはこれを返還することを誓約します。
4. XYZは、契約の履行過程において取得することになるABCの営業秘密、ABCの研究開発・営業・財産等に影響を及ぼしうる有形・無形の情報、その他会社の主要営業資産に関するすべての権利をABCが所有することを認め、これをABCに帰属させることを誓約します。
5. XYZは、契約が期間満了、解約、解除等の何らかの事由により終了する場合、XYZが契約の履行過程において取得したABCの営業秘密、ABCの研究開発・営業・財産等に影響を及ぼしうる有形型・無形の情報、その他ABCの主要営業資産及びこれに関する資料のすべてをABCに返却し、これに関するいかなる形態の写し又は複製物も保有せず、返却できないものは廃棄することを誓約します。
6. XYZは、XYZの役職員に対しても、上記の事項を遵守するよう本誓約書に記載された趣旨の義務を課するなど、必要な措置をとることを誓約します。

XYZは上記の誓約事項に違反する場合、契約の解約、解除及び関連法規による民事・刑事上の責任を負うことを誓約します。

（上記の内容を確認して理解し、これに署名する）

20__ . __ . __ .

誓約者：株式会社 XYZ

（住所） _____

代表取締役 （印）

株式会社ABC御中

1.6 営業秘密管理状況チェックシート

営業秘密名		担当者	
分類	項目	チェックリスト	チェック
制度的 規則	管理規定		
	分類及び指定		
	取扱い		
	生成と取得		
	教育及び訓練		
	アフターケア		
人的 管理	内部者	入社時	
		在職時	
		退職時	
	外部者	取引先	
		協力会社	
	アクセス権者		
物理的 措置	統制区域設定	施錠装置	
		その他	
	コンピュータ 管理	パスワード	
		その他	
	通信セキュリ ティ	外部アクセス	
		内部アクセス	
		バックアップ	
	書類等の管理	秘密表示	
		保管	
		搬出、複製	
		回収及び廃棄	
	電子化された 媒体管理	秘密表示	
		保管	
		搬出、複製	
		回収及び廃棄	
	合計		必須改善項目（ 件）

1.7 その他の書式

(1) 携帯用コンピュータ等の使用者との秘密保持誓約書

秘密保持誓約書 (携帯用コンピュータ等の使用者)

所属：

氏名：

生年月日： ____年 ____月 ____日

私は、株式会社ABC(以下「会社」という。)から営業秘密及び営業資産の重要性と営業秘密等の保護に係る法令及び会社の就業規則、営業秘密管理規程その他の社規、方針、政策等に関する十分な説明を受け、その内容を理解した上で、以下の事項を遵守することを誓約します。

私は、業務遂行のため、会社から以下のような装備の使用許可を受けたことを確認します。

物品の名称/種類： _____

物品管理番号： _____

使用期間： _____

1. 私は、会社が使用を許可した携帯用コンピュータ等情報処理装置(以下、「情報処理装置」という。)、USBメモリ等の電子記録媒体(以下、「電子記録媒体」という。)を業務目的でのみ使用し、パスワード設定等の方法により、その収録された情報が漏洩しないようにすることを誓約します。
2. 私は、情報処理装置及び電子記録媒体を第三者に譲渡するか、又は使用するよう提供せず、これに対する使用、携帯、保管等に相当な注意を払い、その使用中に発生する事項に対する一切の責任を負担することを誓約します。
3. 私は、会社が使用を許可した情報処理装置又は電子記録媒体であっても、会社の許可なく会社の営業秘密に関するいかなる形の資料であっても会社外に持ち出さず、万一持ち出す場合は、会社の事前確認手続き、パスワード設定等の必要なセキュリティ措置を遵守し、これに関するコピーも個人的に保管しないことを誓約します。

4. 私は、使用が許可された期間が満了するか、又はその前であっても、業務上携帯用コンピュータ等を使用する必要がなくなった場合、遅滞なく会社に返却することを誓約します。

上記の誓約事項に違反した場合、関連法規による民事・刑事上の責任を負うことを誓約します。

（上記の内容を確認して理解し、これに署名する）

20__ . __ . __ .

誓約者： （署名）

株式会社ABC御中

(2) 教育履修確認書

教育履修確認書

氏名 _____

所属 _____

役職 _____

私は、株式会社ABC(以下「会社」という。)の役職員として、会社が実施し以下の営業秘密保護教育に参加し、所定の教育を履修したことを確認します。

- ・ 教育日付 : _____
- ・ 教育場所 : _____
- ・ 教育内容 : _____

20__ . __ . __.

株式会社ABC

代表取締役

(印)

(3) 秘密資料・物品返却確認書

営業秘密資料・物品返却確認書

所属：
氏名：
生年月日：20__年__月__日

私は[]年[]月[]日付で株式会社ABC(以下、「会社」という。)を退職するにあたり、私が会社の業務を遂行する過程で取得した会社の営業秘密、その他主要営業資産及びこれに関して私が保有している以下のような資料(コピーを含む)及び物品をすべて会社に返却し、その他会社の営業秘密、その他主要営業資産を保有していないことを確認します。

No.	資料/物品の名称	資料/物品の内容
1		
2		
3		
4		

20__ . __ . __.

誓約者： (署名)

株式会社ABC御中

2. 外部関係用標準書式(1) 外部者との秘密保持契約書の例

2.1 外部者との秘密保持契約書の例

秘密保持契約書

株式会社ABC(以下「ABC」という。)と、株式会社XYZ(以下「XYZ」という。)は、秘密情報の提供に関し、下記のとおり秘密保持契約を締結する。

記

第1条(契約の目的)

本契約は、ABCとXYZが『(業務要旨の記載)(以下「本業務」という。)]に関して、それぞれ相手方に提供する秘密情報を秘密に保持し、保護するために必要な諸事項を規定することを目的とする。

第2条(秘密情報の定義)

①本契約において「秘密情報」とは、ABC又はXYZが本業務の遂行過程で自ら知り得、又は相手方又はその職員(以下「相手方」という。)から提供を受けて知り得た相手方に関する一切の技術上又は経営上の情報及び、これを基に新たに発生した一切の技術上又は経営上の情報をいう。

② 第1項の秘密情報は、書面(電子文書を含む。以下同じ。)、口頭あるいはその他の方法で提供されるすべてのノウハウ、工程、図面、設計、実験結果、サンプル、仕様、データ、公式、製法、プログラム、価格表、取引明細書、生産単価、アイデア等すべての技術上又は経営上の情報とそれらの情報が収録された物又は装備等をすべて含む。

第3条(秘密の表示)

①各当事者が相手方に書面による秘密情報の提供を行う場合、その書面に秘密である旨を示す文句(「秘密」又は「対外秘」等の邦文又は英文で表示)を表示しなければならない。

②各当事者が相手方に口頭や映像又は当事者の施設、装備サンプルその他の品目を観察・調査させる方法で秘密情報を提供する場合には、直ちに相手方に当該情報が秘密情報に属することを告知しなければならない。この時、秘密情報を提供した当事者は、秘密情報提供日から15日以内に相手方に当該情報が秘密情報に属する旨の書面を発送しなければならない。

第4条(情報の使用用途及び情報取扱者の制限)

①各当事者は、相手方の秘密情報を「本業務」の遂行又は「本業務」に係る契約で定めた本来の目的にのみ使用すべきである。

② 各当事者が「本業務」の遂行のため相手方の秘密情報を第三者に提供する際は、事

前に相手方から書面による同意を得なければならない、その第三者との間で当該秘密情報の保持及び保護を目的とする別途の秘密保持契約を締結した後に、その第三者に当該秘密情報を提供しなければならない。

③ 各当事者は、直接的・間接的に「本業務」を遂行する役職員に限り、相手方の秘密情報を取り扱うことができるよう必要な措置を取らなければならない。当該役職員それぞれに相手方の秘密情報に対する秘密保持義務を周知させなければならない。その際、相手方は他の当事者に対し、当該役職員から秘密保持誓約書の提出を受けるなどして、当該情報の秘密性を保持するために必要な措置を求めることができる。

第5条(秘密保持義務)

① 各当事者は、相手方の書面承諾なしに、秘密情報を含め、本契約の締結事実や内容、「本業務」の内容などを公表、又は第三者に通知してはならない。ただし、客観的な証拠を通じて以下の各号に該当することが立証される情報は、秘密情報でないか、秘密保持義務がないものとみなす。

1. 相手方の秘密情報提供前に他の当事者がすでに知っているか、又は知りうる情報
2. 秘密情報の提供を受けた当事者の故意又は過失によらず公知の事実となった情報
3. 秘密情報の提供を受けた当事者が適法に第三者から提供を受けた情報
4. 秘密情報の提供を受けた当事者が秘密情報と関係なく独自に開発、又は知り得た情報
5. 第3条第2項により秘密情報であることを告知しないか、又は秘密情報に属する旨の書面を発送していない情報
6. 法院その他公共機関の判決、命令又は関連法令に基づく公開義務に従って公開した情報

② 各当事者が第1項第6号に従い情報を公開する場合には、あらかじめ相手方にその旨を書面で通知し、相手方が適切な保護及び対応措置ができるようにしなければならない。

第6条(資料の返還)

①各当事者は、相手方の要請があれば、いつでも相手方の秘密情報が記載されているか、又はこれを含む諸資料、装備、書類、サンプル、その他の有体物(コピー、複写物、模倣物、模倣装備などを含む)を直ちに相手方に返還するか、又は相手方の選択に従いこれを廃棄し、その廃棄を証明する書類を相手方に提供しなければならない。

②第1項の資料の返還又は廃棄に要する費用は、各当事者が均等に負担するものとする。ただし、資料の返還又は廃棄の義務者が、まずその費用を支出した後、相手方にその負担部分を精算して請求するものとする。

第7条(権利の不存在等)

- ① 本契約に基づいて提供される秘密情報に関するすべての権利は、これを提供した当事者に属する。
- ② 本契約は、いかなる場合であっても、秘密情報の提供を受ける者に対して秘密情報に関する何らかの権利や使用权を付与するものとは解釈されない。
- ③ 本契約は、いかなる場合であっても、当事者間において今後何らかの確定的な契約の締結、製造物の販売や購入、実施権の許諾などを暗示又は強制せず、その他本契約の当事者が秘密情報に関して他の第三者と何らかの取引や契約関係に入ることを禁止又は制限しない。
- ④ 秘密情報の提供者は相手方に秘密情報を提供する適法な資格があることを保証する。
- ⑤ 各当事者は、本契約の目的のために相手方の施設を訪問したりこれを利用する場合は、相手方の諸規定及び指示事項を遵守しなければならない。

第8条(契約期間)

- ① 本契約は、本契約の締結日から[]年間その効力を有する。
- ② 第1項に関わらず、本契約第4条、第5条及び第7条の義務は、本契約の契約期間が満了するか、又は本契約が解除・解約などの事由により終了した後から引き続き有効に存続するものとする。

第9条(損害賠償、違約罰)

- ① 本契約に違反した当事者は、これにより相手方が被った全ての損害を賠償しなければならない。
- ② 本契約に違反した当事者は、第1項の損害賠償と別に、相手方に違約罰として金[]ウォンを支払わなければならない。

第10条(権利義務の譲渡、契約の変更)

- ① 各当事者は、相手方の書面による事前の同意なしに本契約上の権利義務を第三者に譲渡、又は移転してはならない。
- ② 本契約の修正や変更は、両当事者の正当な代表者が記名押印又は署名した書面合意によってのみ行われる。

第11条(契約の分離可能性)

本契約のある規定が法院によって違法、無効又は執行不可能と宣言される場合でも、これは本契約の残りの規定の有効性に影響を及ぼさない。

第12条(紛争の解決)

本契約に関連して紛争が発生した場合、当事者の相互協議による解決を模索するが、紛争に関する合意がなされない場合には、[ソウル中央地方法院]を第1審管轄法院とし、訴訟を通じて紛争を解決することとする。

「ABC」と「XYZ」は、本契約の成立を証明するために、本契約書2部を作成し、それぞれ

れ署名（又は記名押印）の上、それぞれ1部ずつ保管する。

20____年 ____月 ____日

“ABC”

（名称）_____

（住所）_____

（代表者）_____

“XYZ”

（名称）_____

（住所）_____

（代表者）_____

2.2 紛争対応に関する書式

(1) 営業秘密侵害予防に関する通知書

通知書

受信:株式会社XYZ

参照:代表取締役

件名:営業秘密侵害予防促しの件

1. 貴社ますますご清栄のこととお慶び申し上げます。
2. 貴社に入社した下記の職員は、従前弊社で下記のように在職中に、職務に関して弊社の営業秘密を取得し、これに関して弊社は、下記の職員の退職時に、営業秘密保護誓約書の提出を受けました。

氏名	
所属	
役職	
在職期間	
担当業務	

3. よって、貴社で上記の職員が貴社の業務を遂行する過程で、弊社の営業秘密を侵害することがないように注意を促す次第でございます。

20__ . __ . __.

株式会社ABC

代表取締役

(印)

(2) 営業秘密侵害中止要請通知書

通知書

受信:株式会社XYZ
参照:代表取締役
件名:営業秘密侵害予防促しの件

1. 貴社ますますご清栄のこととお慶び申し上げます。
2. 貴社に入社した下記の職員は、従前弊社で下記のように在職中に、職務に関して弊社の営業秘密を取得し、これに関して弊社は下記の職員の退職時に、営業秘密保護誓約書の提出を受けました。

氏名	
所属	
役職	
在職期間	
担当業務	

3. よって、貴社で上記の職員が貴社の業務を遂行する過程で、弊社の営業秘密を侵害することがないように注意を促す次第でございます。

20__ . __ . __.

株式会社ABC
代表取締役 (印)

(3) 合意書(紛争終結合意時)

合意書

株式会社ABC(以下「ABC」という。)と株式会社XYZ(以下「XYZ」という。)は、XYZの営業秘密侵害事件を円満に解決するため、以下のとおり合意する。

1. XYZは、ABCが開発した []に関する営業秘密(以下「本件営業秘密」という。)を侵害し、xyz製品(以下「侵害製品」という。)を生産及び販売したことを認める。
2. XYZは、本合意書を作成した日から侵害製品を生産、販売、輸出、譲渡及びこれに関する広告をしてはならない。ただし、XYZが本合意書を作成する前日まで生産した侵害製品は、ABCの数量確認及び書面承認を受けて 年 月 日まで販売、輸出及び譲渡ができ、その期間が経過したときはABCの確認を受けて廃棄しなければならない。
3. XYZは、 年 月 日までにABCに本件営業秘密の侵害に対する損害賠償として金[]ウォンを支払わなければならない。もしこれを遅滞するときは、その遅滞日数に対して上記の金員に年[5]%の率による遅延利息を加えて支払わなければならない。
4. XYZが本合意に違反して侵害製品を生産、販売、輸出、譲渡及び広告したときは、損害賠償と別途で、本合意に違反して生産、販売、輸出又は譲渡した侵害製品1つにつき金[]ウォンを、本合意に違反して広告した場合にその違反行為1回につき金[]ウォンを違約罰としてABCに各支払わなければならない。

20__年 __月 __日

“ABC”

(名称) _____

(住所) _____

(代表取締役) _____ (印)

“XYZ”

(名称) _____

(住所) _____

(代表取締役) _____ (印)

(4) 合意書(技術料支払合意時)

合意書

株式会社ABC(以下「ABC」という。)と株式会社XYZ(以下「XYZ」という。)は、XYZの営業秘密侵害事件を円満に解決するため、以下のとおり合意する。

1. XYZは、ABCが開発した[]に関する営業秘密(以下、「本件営業秘密」という。)を侵害し、[]製品(以下、「侵害製品」という。)を生産及び販売したことを認め、これに対する損害賠償として[]年[]月[]日までにABCに金[]ウォンを支払うものとし、もしこれを遅滞するときは、その遅延日数に対して上記の金員に年[5]%の率による遅延利息を加えて支払うものとする。
2. XYZは、本合意書を作成した日から[]年間適法に侵害製品を生産、販売、輸出及び広告することができる。
3. XYZは、第2項の期間(以下「合意期間」という。)に販売した侵害製品(返品又は戻入された侵害製品の数量は除くが、広告、宣伝のために無償で提供した侵害製品の数量は含む)1個につき金[]ウォンを技術料としてABCに支払うものとするが、合意期間に、毎年6月30日と12月31日を基準に技術料を精算し、毎年1月1日から6月30日まで販売した数量については毎年7月31日に、毎年7月1日から12月31日まで販売した数量については、その翌年1月31日までにそれぞれ支払うものとする。
4. ABCは、XYZの侵害製品販売数量に対して異議があるときは、XYZの売上資料、その他会計資料を閲覧及び調査することができ、XYZは、ABCの会計資料閲覧及び調査に協力しなければならない。この際、ABCは公認会計士を委嘱し、XYZの売上資料、その他の会計資料を閲覧及び調査させることができ、XYZはこれに対して異議を唱えることができない。
5. XYZ又はXYZの役員及び被用者が本件営業秘密を改良、拡張、代替、追加等の方法により開発した技術(以下「改良技術」という。)に関する新たな特許、実用新案等知的財産権を取得しようとする場合には、事前にABCに書面でその事実を通知しなければならない。その改良技術に関する知的財産権はABCとXYZの共有とし、その出願、登録、維持費用は、ABCとXYZの共同負担とする。
6. XYZがABCに支払った第1項及び第3項の金員は、本件営業秘密に関するいかなる事由によっても返還を請求することができない。

7. ABCは、XYZが実施する本件営業秘密が第三者の権利を侵害しないか、又は事業化、商用化が可能であることを保証するものではなく、本件営業秘密の実施によりXYZに発生したいかなる損失(第三者に対する実施料支払いを含む)についても責任を負わない。
8. ABCとXYZは、XYZの本件営業秘密侵害に関し、本合意により全ての紛争を清算し、一切の民事・刑事上の異議を提起しないこととする。

20__年 __月 __日

“ABC”

株式会社ABC

(住所) _____

(代表取締役) _____ (印)

“XYZ”

株式会社XYZ

(住所) _____

(代表取締役) _____ (印)

3. 営業秘密保護規定

3.1 営業秘密管理規定

営業秘密管理規定

第1章 総則

第1条（目的）

この規定は株式会社ABC（以下「会社」という。）の情報資産、セキュリティ事項、営業秘密及びその他知的財産権の管理及び保護に関する必要な事項を定め、会社の発展を図ることを目的とする。

第2条（定義）

この規定で使用される用語の定義は、以下のとおりである。

1. 「情報」とは、会社の経営又は活動に必要な一切の知識をいう。
2. 「情報資産」とは、「情報及び情報システム」を包括した概念をいう。
3. 「情報システム」とは、会社が保有しているコンピュータ、電算システム、ネットワーク、ソフトウェア及び各種映像媒体施設物等、「情報」を管理するのに必要な全ての資産をいう。
4. 「営業秘密」とは、会社が保有又は保有する情報として公然と知られておらず、独立した経済的価値を有するものであり、合理的努力により秘密に保持された生産方法・販売方法その他営業活動に有用な技術上又は経営上の情報をいう。
5. 「知的財産権」とは、人間の創造的活動又は経験によって創出され、又は発見された知識・情報・技術、思想や感情の表現、営業や物の表示、生物の品種や遺伝資源、その他無形のものであって、財産的価値が実現できることに関する権利をいう。
6. 「役職員」とは、会社に在職する役員と職員をいう。

第3条（セキュリティ業務の分類）

①会社のすべての「情報」について、「一般業務」と「セキュリティ業務」とに区分し、「セキュリティ業務」はさらに「システムセキュリティ業務」と「一般セキュリティ業務」とに区分される。

②「システムセキュリティ業務」は、コンピュータ、情報通信ネットワーク等、主としてコンピュータを介して行われる情報システムに関するセキュリティ業務をいい、「一般セキュリティ業務」とは、それ以外の全ての部門の情報セキュリティ業務をいう。

第4条(適用範囲、保護対象)

①この規定は、会社で新規採用・在職・退職するすべての役職員と外部協力会社とパートナー、その他会社に入出入りするすべての人に適用する。

②この規定は会社が保有している以下の各号をその保護対象とする。

1. 営業秘密そのもの
2. 営業秘密が化体された物及び物体(例:書類、図面、複写物、磁気テープ、コンピュータ、CD、DVD、USB、外付けHDD、電話機、資材、生産品等)
3. 営業秘密生産設備と装備
4. 営業秘密統制区域
5. 知的財産権
6. その他会社機密に関する情報資産

第2章 営業秘密の保護管理

第5条(セキュリティ業務の組織及び機能)

①会社は、営業秘密その他情報資産の管理と保護のために、会社内のすべてのセキュリティ業務を総括担当するセキュリティ管理責任者を指定する。

②セキュリティ管理責任者の職務は、以下の各号のとおりである。

1. 部署別営業秘密保護及び管理に関する計画樹立及び調整
2. 所管営業秘密の等級分類
3. 営業秘密に関する教育の実施
4. 営業秘密保有現況調査及び管理監督
5. 秘密保持契約及び誓約書等の執行
6. セキュリティ関連規定及び指針の樹立・調整
7. その他会社の営業秘密保護その他セキュリティに関して必要な事項

③セキュリティ管理責任者は四半期別に代表取締役等にセキュリティ業務の現況を報告しなければならない。役職員が重要な営業秘密を開発又は創出した場合も同様とする。

④会社の各部署長は部署業務に関する営業秘密(第6条の一級秘密を除く)の管理責任者として、第2項第1号から第5号及び第7号の職務を遂行する義務と責任を有する。

⑤セキュリティ管理責任者は、各部署長とセキュリティ業務に関する協力体制を樹立し、社内の主要なセキュリティ状況を共有し、必要な事項については全役職員に告知する。

第6条(営業秘密の分類と基準)

①会社は営業秘密について、その重要性和価値の程度によって「一級秘密」「二級秘密」「三級秘密」の3段階に分類し、必要に応じてその分類を変更することができる。

②「一級秘密」とは、競合他社又は対外に流出する場合、会社が莫大な損害を被り得る以下の各号の営業秘密をいう。

1. 会社の基盤技術及びこれに対する知的財産権の出願に関する事項
 2. 世界超一流技術、国防・安保関連技術又は国家コア技術に関する事項
 3. 会社の営業戦略、M&Aその他会社の重要営業秘密に該当する事項
- ③「二級秘密」とは、競合他社又は対外に流出した場合、会社に被害を与えかねない営業秘密のうち、「一級秘密」に該当しない営業秘密をいう。
- ④「三級秘密」とは、「一級秘密」又は「二級秘密」ではない「営業秘密」をいう。
- ⑤営業秘密は、以下の各号の期間保存する。ただし、会社のセキュリティ管理責任者又は各部署長は各営業秘密の特性を考慮して、以下の第2号、第3号の保管期間より長期間を保存期間として指定することができる。
1. 一級秘密:永久保存
 2. 二級秘密:10年 3. 三級秘密:5年

第7条(営業秘密の表示及び保管)

- ①営業秘密は、その表紙に「対外秘」の表示と共に、各等級によって以下のように区分して表示しなければならない。
1. 一級秘密:対外秘|1級
 2. 二級秘密:対外秘|2級
 3. 三級秘密:対外秘|3級
- ②営業秘密が化体された書類、物等は、一般文書、物と分離して、別途の保存箱、金庫等セキュリティ装置を備えた容器に入れ、特別に管理しなければならない。
- ③ 営業秘密が含まれている電子文書は、一般の電子文書と分離して、パスワードを設定し、営業秘密取扱資格がある者以外は閲覧できない方法で保管しなければならない。

第8条(営業秘密統制区域の設定)

- ①営業秘密の保護と、重要施設装備及び資材の保護のために、必要な場合、一定の範囲を統制区域に指定し、必要に応じてCCTV及び施錠装置その他の統制区域を保護するための装置又は設備を設置する。
- ②第1項の統制区域には、外部から認識できる適切な方法により「統制区域」である旨を表示し、会社から事前に許可を受けた関係者以外の出入りを統制しなければならない。
- ③第1項の統制区域には出入者名簿を備え、出入者を記録・保存しなければならず、必要な場合には出入者から営業秘密保護に関する覚書又は誓約書を徴求しなければならない。

第9条(管理台帳)

各営業秘密の管理責任者は、第7条第2項により管理している営業秘密について、等級別に別紙第1号書式の営業秘密管理台帳(以下「管理台帳」という。)を備え、変動事項等に関する記録を維持・管理しなければならない。

第10条(取扱資格)

第6条により分類された営業秘密の取扱資格は、以下の各号のとおりである。

1. 一級秘密:代表取締役、代表取締役が指定した役職員、セキュリティ管理責任者
2. 二級秘密:1級秘密取扱者、当該営業秘密が属する担当部署の部署長及び実務担当者
3. 三級秘密:2級秘密取扱者に同じ

第11条(セキュリティ点検)

①セキュリティ管理責任者は、営業秘密を取り扱う各部署に対して定期的にセキュリティ点検を実施しなければならない。

②セキュリティ管理責任者は、営業秘密保護のために必要な場合は、代表取締役にその理由を報告した上で、特定の役職員及び部署を選定し、抜き打ちでセキュリティ点検を実施することができる。

第12条(復旧)

各営業秘密の管理責任者は、営業秘密に対する危険が発生し、又は発生するおそれがあることを知ったときは、遅滞なくセキュリティ管理責任者及び関連部署にこれを通報し、直ちに必要な措置をとらなければならない。

第13条(物品の搬入、搬出)

①会社の資産及び物品を搬入・搬出する役職員は、管理責任者又は関連部署長の事前承認を得なければならない。

②コンピュータ等情報処理装置(携帯用を含み、以下「コンピュータ」という。)及びUSBメモリ、外付けHDD等電子記録媒体(以下「電子記録媒体」という。)等を使用する役職員は、事前にセキュリティ管理責任者又は担当部署長の承認を得なければならず、会社の業務のためにのみ使用すべきである。

③コンピュータ又は電子記録媒体を搬入・搬出する場合、これの使用者は関連規定に従い、搬入・搬出日、機器仕様、使用用途、使用者情報等を作成して担当部署長に提出し、担当部署長はこれを直接確認した後、使用者が提出した書類をセキュリティ管理責任者に提出しなければならない。

④セキュリティ管理責任者は、第3項の書類を別途保管し、社内のコンピュータ及び電子記録媒体等の存在及び使用状況を随時確認しなければならない。

第14条(非常対策)

①営業秘密管理責任者は、火災又は自然災害等の非常状況に備えて、コピーの作成が必要な営業秘密については、セキュリティ管理責任者と協議の上、コピーを作成し、これを別の場所に保管して定期的に管理しなければならない。

②セキュリティ管理責任者は、火災や自然災害及び会社の機密流出等の非常状況発生時、会社の被害を最小限に抑えるための関連規定及び指針を樹立し、これを全役職員に告知しなければならない。

第3章 営業秘密の生成と取得

第15条(営業秘密の創出及び帰属)

役職員が職務に関して研究・開発又は取得した営業秘密は会社の所有であり、当該役職員はこれを会社に帰属させなければならない。ただし、役職員が自らの一般的知識、経験、技術に基づいて創出した営業秘密については、特別の約定又は規定がある場合には、その約定又は規定に従い、その約定又は規定がない場合には当該役職員の所有とする。

第16条(営業秘密の申告)

- ①役職員が在職中に営業秘密を創出した場合には、関連部署の長に申告しなければならない。
- ②役職員が本規定の適用を受けない他人と共同で会社の業務に関する営業秘密を創出した場合も、第1項の規定により申告しなければならない。

第17条(報奨)

役職員が創出した営業秘密の中でこれによって会社の利益が発生し、相当の価値がある営業秘密に対しては、職務発明に準じて報奨金を支払わなければならない。

第18条(取得)

役職員が営業秘密を外部から取得した場合、関連部署の部署長に申告し、関連部署の部署長は、これを管理台帳に記載して役職員が創出した営業秘密と同じ方法で管理する。

第4章 営業秘密の使用

第19条(使用)

- ①会社の営業秘密は、第10条に基づき営業秘密取扱資格が認められる営業秘密管理責任者の承認を得て使用することができる。
- ② 会社の営業秘密を使用又はこれを搬出する場合は、事前に営業秘密管理責任者に申請しなければならない。上記の管理責任者は申請人の営業秘密取扱資格を確認した後、その資格が認められる場合に限り、別紙第2号書式の営業秘密使用台帳(以下「使用台帳」という。)に申請内訳を記載の上、当該営業秘密を搬出、又は使用するようしなければならない。この際、第一級秘密の使用又は搬出については、あらかじめセキュリティ管理責任者の同意を得なければならない。

第20条(譲渡)

- ①営業秘密を譲渡する際は、関連部署と協議をして、営業秘密管理責任者、セキュリティ管理責任者及び代表取締役の承認を得なければならない。
- ②営業秘密管理責任者は、営業秘密を譲渡した後も、必要に応じて関係記録を廃棄せず、営業秘密の保持・管理を行わなければならない。

第21条(部署間での使用)

会社内部の部署間で営業秘密を貸与・使用・流通のために移送する際は、第19条により部署責任者間で引継手続きを経なければならず、営業秘密を移送された部署の責任者は、当該営業秘密の使用が終了するときは、直ちに引受手続きを経て、当該営業秘密を元々保管していた部署に返還しなければならない。

第22条(移送方法)

①営業秘密を社内で貸与・使用・流通のために移送する際は、密閉包装や容器等を使用しなければならない。

②やむを得ず営業秘密を通信手段によって移送するときは、セキュリティが設定されたファイル等を使用し、又は主要内容部分は、これを分離して移送するなど必要なセキュリティ措置をとらなければならない。

第23条(管理・廃棄)

①会社の営業秘密は別表1. 営業秘密別管理基準に従って管理する。

②これ以上活用価値のない営業秘密は一定の手続きによって廃棄することができ、廃棄後も必要な場合は引き続き保護・管理する。

第5章 役職員の営業秘密保護義務

第24条(入社時)

会社が新規に採用した役職員に対しては、別紙第3号の秘密保持誓約書を作成し、提出するようにする。

第25条(在職中の営業秘密漏洩禁止)

①役職員は在職時に取得した営業秘密に対しては、この規定に基づいて取り扱い・管理しなければならない。許可なくこれを流出・公開又は使用してはならない。

②研究開発の結果、新製品等を発表したり展覧会等に出品してやむを得ず営業秘密を開示することになる場合は、事前に当該営業秘密の管理責任者及びセキュリティ管理責任者の承認を得なければならない。

③会社は、役職員の在職中に定期的に別紙第4号の秘密保持誓約書を徴求することができ、プロジェクトへの参加など必要な際は別紙第5号の秘密保持誓約書を徴求することができる。

第26条(退職時)

①会社の役職員であった者は、会社の事前承認なく、在職時に取得した営業秘密を公開・流出又は使用してはならない。

②役職員が退職する場合、その役職員が保有しているすべての営業秘密を返納してもらい、別紙第6号書式の秘密保持誓約書を徴求しなければならない。

第6章 協力会社等に対する秘密管理

第27条(協力会社その他第三者)

協力会社その他第三者に営業秘密を提供し、又は営業秘密に関する業務を行わせる場合には、当該協力会社その他第三者に別紙第7号書式の秘密保持誓約書を作成させ、提出させなければならない。

第28条(共同プロジェクト、技術提携契約)

- ①会社が外部機関等に研究開発プロジェクトを依頼、又は外部機関との間で技術提携契約を締結するにあたり、会社の営業秘密を開示しなければならない場合、外部機関の参加役職員には別紙第8号書式の秘密保持誓約書の提出を受け、外部機関との間では別紙第9号書式の秘密保持契約を締結した上で、営業秘密を開示するものとする。
- ②会社は外部機関との協議により、第1項の第8号書式又は第9号書式の内容の一部を変更することができる。

第7章 システムセキュリティ管理

第29条(コンピュータの使用)

- ①社内のすべてのコンピュータ使用者はソフトウェアの違法コピーを使用してはならず、ソフトウェアの違法コピーを使用することによるすべての責任は使用者本人にあり、会社は責任がない。
- ②社内の全てのコンピュータ使用者は、ウイルス侵入及びハッキングを防止するためのソフトウェアと各種セキュリティソリューションをインストールして、定期的にバックアップ及びアップデート管理をしなければならない。

第30条(通信ネットワークの使用)

- ①役職員は会社内で共通で使用する通信ネットワークのみを使用しなければならない。
- ②セキュリティ管理部署及びセキュリティ管理責任者は、会社の営業秘密保護及び業務の効率性確保のため、インターネット上の特定サイトへのアクセスを統制することができる。
- ③役職員は会社で使用を禁止したEメールを使用してはならない。
- ④役職員は外部に文書を発送する場合には部署長の事前承認を受けなければならない。ただし、専決権のある役職員は、この限りでない。

第31条(システム管理)

- ①セキュリティ管理責任者は、会社のセキュリティシステムを年1回以上定期的に点検し、その結果を全役職員に対して告知する。
- ②役職員は会社のセキュリティシステムに対する問題を発見次第、セキュリティ管理責任者にその事実を申告しなければならない。
- ③システムセキュリティについては、この規定によるほか、別途規定するところによる。

第8章 営業秘密侵害救済

第32条(救済措置)

- ①セキュリティ管理責任者及び各部署長は、会社の営業秘密を侵害された際は、遅滞なく関係法令及び社規による必要な救済措置を取らなければならない。
- ②セキュリティ事故発生時、業務担当者とセキュリティ管理責任者等の関係者は、事件の調査及び解決に誠実に協力しなければならない。

第33条(営業秘密漏洩者に対する懲戒)

営業秘密漏洩者に対しては、第29条の規定による措置を取るとともに、別途社規により懲戒することができる。

第34条(関連者に対する懲戒)

営業秘密漏洩を不注意又は過失で知り得なかったか、又は防げなかった関係者に対しても、社規により懲戒することができる。

第9章 補則

第35条(教育)

- ①セキュリティ管理責任者は、全役職員に対して定期的に営業秘密に関する教育を行わなければならない。
- ②営業秘密教育は外部に委託して行うことができる。

付則

1. この規定は、20 年 月 日から施行する。
2. この規定の施行前から保有している営業秘密のうち、主要営業秘密については、規定施行後1ヶ月以内に等級分類(再分類)をして等級を指定(再指定)する。

1. 「一級秘密」を記録した文書、図面、写真、書籍、磁気テープ、FD、CD、コンピュータサーバ等(以下「記録媒体」という。)の取扱いは、以下のとおりとする。

(1) 保管

- ・記録媒体は、営業秘密管理台帳に記録媒体の要旨を記入した後、他の文書と区別して、施錠装置のある保存箱に厳重に保管しなければならない。その際、鍵等は管理責任者が保管する。
- ・電子化された情報を情報システム機器に保管する場合は、暗号化等の適切な措置を取り、当該情報システム機器を統制区域内に設置する。もし当該情報システム機器を統制区域内に設置できない場合は、管理責任者は、他人のアクセスを防止するための最善のセキュリティ措置をとらなければならない。
- ・電子化された情報を外部記録媒体に保管する場合、暗号化等の適切な措置を取り、当該外部記録媒体を施錠装置のある保存箱等に厳重に保管しなければならない。その際、

鍵等は管理責任者が保管する。

(2) 閲覧

- ・管理責任者の許可なく記録媒体を閲覧することができない。
- ・当該情報へのアクセスの許可を受けていない者は記録媒体を閲覧することができない。
- ・電子化された情報の画面表示は、入室制限され当該情報の保有者が実在する場所において、他人に見えないように格別の注意を払って行われなければならない。
- ・管理責任者は営業秘密使用台帳に閲覧者名、日時等を記録する。

(3) 複製

- ・管理責任者の許可なく記録媒体を複製できない。このとき、複製物は原本と同等に「一級秘密」として扱わなければならない。
- ・電子化された情報の複製は管理責任者のみが実施できる。
- ・管理責任者は営業秘密使用台帳に複製者名、日時、目的等を記録する。

(4) 搬出

- ・管理責任者の許可なく記録媒体を搬出することができない。
- ・管理責任者の許可がある場合でも、許可を受けた本人のみが記録媒体を所持し、漏洩及び紛失の責任を負うこととする。
- ・管理責任者は営業秘密使用台帳に搬出者名、日時、目的、返却時期等を記録する。

(5) 廃棄

- ・記録媒体は、使用後、記録媒体を配付された者の責任の下、適切な方法により廃棄するものとする。
- ・電子化された情報は、管理責任者の承認を得て、第三者が残留情報を解読できないように必要な措置をとった後に廃棄するものとする。
- ・管理責任者は営業秘密管理台帳に廃棄日時等を記録する。

2. 「二級秘密」記録媒体の取扱いは、以下のとおりとする。

(1) 保管

- ・記録媒体は営業秘密管理台帳に記録媒体の要旨を記入した上で、他の文書と区別して、施錠装置のある保存箱に厳重に保管しなければならない。その際、鍵等は管理責任者が保管する。
- ・電子化された情報を情報システム機器に保管する場合には、暗号化等の適切な措置を取り、当該情報システム機器を統制区域内に設置する。もし当該情報システム機器を統制区域内に設置できない場合は、管理責任者は、他人のアクセスを防止するための最善のセキュリティ措置をとらなければならない。
- ・電子化された情報を外部記録媒体に保管する場合、暗号化等の適切な措置を取り、当該外部記録媒体を施錠装置のある保存箱等に厳重に保管しなければならない。その際、

鍵等は管理責任者が保管する。

(2) 閲覧

- ・記録媒体は重大な必要性が認められる場合には、記録媒体所持者の責任の下、関係者に閲覧させることができる。
- ・電子化された情報の画面表示は、他人に見えないように注意を払って行われなければならない。
- ・管理責任者は営業秘密使用台帳に閲覧者名、日時等を記録する。

(3) 複製

- ・記録媒体は重大な必要性が認められる場合、記録媒体所持者の責任の下に複製することができる。ただし、複製物は原本と同等「二級秘密」として扱わなければならない。
- ・電子化された情報の複製は、管理責任者の承認を得て、記録媒体を配付された者の責任の下に行うことができる。
- ・管理責任者は営業秘密使用台帳に複製者名、日時、目的等を記録する。

(4) 搬出

- ・業務上の必要性が認められた場合にのみ記録媒体を搬出することができる。
- ・この場合、記録媒体を搬出した本人が記録媒体を所持するようにし、漏洩及び紛失の責任を負うこととする。
- ・管理責任者は営業秘密使用台帳に搬出者名、日時、目的、返却時期等を記録する。

(5) 廃棄

- ・記録媒体は、使用後、記録媒体を配付された者の責任の下に、適切な方法により廃棄するものとする。
- ・電子化された情報は、第三者が残留情報を解読できないように必要な措置を取った上、廃棄するものとする。
- ・管理責任者は営業秘密管理台帳に廃棄日時等を記録する。

3. 「三級秘密」記録媒体の取扱いは、以下のとおりとする。

(1) 保管

- ・記録媒体は営業秘密管理台帳に記録媒体の要旨を記入した上、他の文書と区別して保管しなければならない。
- ・電子化された情報を情報システム機器に保管する場合は、暗号化等の適切な措置をとる。
- ・電子化された情報を外部記録媒体に保管する場合、暗号化等の適切な措置を取り、当該外部記録媒体を施錠装置のある保存箱等に厳重に保管しなければならない。その際、鍵等は管理責任者が保管する。

(2) 閲覧

電子化された情報の画面表示は、他人に見えないように注意を払って行われなければならない。

(3) 複製

- ・記録媒体は重大な必要性が認められる場合、記録媒体所持者の責任の下に複製することができる。
- ・電子化された情報の複製は、重大な必要性が認められる場合に限り、記録媒体を配布された者の責任の下で行うことができる。
- ・管理責任者は営業秘密使用台帳に複製者名、日時、目的等を記録する。

(4) 搬出

- ・記録媒体を搬出した本人のみが記録媒体を所持するようにし、流出及び紛失の責任を負うこととする。
- ・管理責任者は営業秘密使用台帳に搬出者名、日時、目的、返却時期等を記録する。

(5) 廃棄

- ・記録媒体は、使用後、済記録媒体を配付された者の責任の下に、適切な方法により廃棄するものとする。
- ・電子化された情報は、第三者が残留情報を解読できないように必要な措置を取った後、廃棄するものとする。
- ・管理責任者は営業秘密管理台帳に廃棄日時等を記録する。

3.2 システムセキュリティ規定

システムセキュリティ規定

第1条(目的)

この規定は、会社の情報システムと情報通信のセキュリティに関する必要な事項を定め、会社の発展を図ることを目的とする。

第2条(用語の定義)

この規定において使用する用語の定義は、以下の各号のとおりである。

1. 「電算室」とは、業務用電算設備及び共用ネットワーク設備が保管される場所をいう。
2. 「システム管理者」とは、業務及び研究目的として保有している情報通信システムの運用及び管理責任を有する該当部署の部署長をいう。
3. 「ホームページ」とは、会社の代表ホームページ及び会社の業務に関連して制作して、対外サービスを行うすべてのものをいう。
4. 「情報セキュリティ、情報保護」とは、情報通信手段により処理、保存、疎通される情報を保護するか、又はハッキング等外部脅威から脆弱要因を除去するための各種手段及び方法をいう。
5. 「情報通信システム」とは、業務処理又は研究目的の遂行のためにネットワークに接続し、多数の人員が利用するサーバ及び情報通信設備をいう。
6. 「補助記録媒体」とは、ディスク、移動型ハードディスク (HDD)、USBメモリ、CD(CompactDisk)、DVD(DigitalVersatileDisk)、携帯電話等資料を保存できる一切のものであって、パソコン等の情報通信システムと分離できる記憶装置をいう。

第3条(システムセキュリティの範囲)

システムセキュリティ管理は、以下の各号のとおりとする。

1. 電算室のセキュリティ
2. 情報資料
3. パソコン(デスクトップ、ノートパソコン、タブレット、スマートフォンなど)
4. 電子メール及び有無線通信ネットワーク
5. ホームページなど公開用ウェブサーバー、SNS(ブログなど)の管理
6. 無線LAN
7. 情報通信ネットワークの新・増設及び情報システムの交替等を行う場合のセキュリティの検討
8. その他のシステムセキュリティ業務に関する事項

第4条(電算室保護対策) 電算室運営部署長は、電算室を制限区域とし、以下の各号の対策を講じなければならない。

1. 防災対策及び外部からの危害防止
2. 電算資料又は装備別取扱者指定運営
3. 常時利用する出入口は1ヶ所と定め、二重ドアとセキュリティ装置を設置
4. その他の電算業務非関連者の立入制限等

第5条(情報資料セキュリティ管理)

①システム管理者は、電算資料及びセキュリティが要求されると判断する電算資料の流出、破壊又は変造等に備えて、以下の各号のように保護対策を講ずる。

1. 電算資料保有現況の管理
2. 装備の搬入・搬出を統制
3. 情報通信ネットワークへの不法アクセス及びコンピュータウイルス被害の予防
4. 重要資料のバックアップ体系の樹立・施行
5. 最新ソフトウェアセキュリティパッチ(patch)の適用

②システム管理者は人為的又は自然的な原因による情報通信システムの障害発生に備えて、システム二元化、バックアップ管理、復旧など総合的なトラブル復旧対策を樹立・施行しなければならない、トラブル復旧システムは以下の各号のとおりである。

1. 重要資料の二重バックアップシステムの構築
2. サーバと物理的に離隔された場所に別途のバックアップシステムを構築
3. リアルタイムバックアップシステムの構築

③システム管理者は、情報通信システムを利用するための使用者アカウントを発行し、非認可者に不必要なサービスを許可しないよう、セキュリティ機能を設定しなければならない。

④ システム管理者はパスワードなど使用者識別及び認証がない使用者アカウントは使用できないようにし、退職時に使用者アカウントを直ちに閉鎖する。

⑤ 主要情報通信システムのオペレーティングシステムに直接アクセスできる権限は、システム管理者にのみ許容し、一般使用者アカウントの付与は制限する。

⑥ 一般使用者による情報通信システム保有資料の利用は、システム管理者が許可したアプリケーションソフトウェアを通じて利用することを原則とし、業務別、資料別の重要度に応じて使用者別にアクセス権限を付与しなければならない。

⑦システム管理者は、非認可者の情報通信システムへの侵入事実を認知した場合、システム保護のためのアクセス遮断など初動措置を取り、電算部署長に連絡し、電算担当部署長は代表取締役及びセキュリティ管理責任者に報告しなければならない。

⑧ システム管理者は、情報通信システムに対して外部業者の遠隔メンテナンス作業を許容してはならない。ただし、やむを得ない場合、必要なセキュリティ対策を講じてから許容することができ、その際も遠隔メンテナンスの内容を確認監督し、必ず記録として保持しなければならない。

⑨ 主要情報通信システムは、システム管理者が一点検しなければならない、点検内容は、以下の各号のとおりである。

1. 装備の全般的な運営状態の点検
2. 装備障害発生 of 事前防止のための予防点検
3. 装置ログ分析及びその結果による適切な対処

4. ソフトウェアの適正な活用の有無、ソフトウェアの違法コピーのインストール有無、セキュリティパッチの適用、バージョンのアップグレードを遂行及び点検
5. 障害が発生、又は障害が発生する恐れがある場合、適切な対処又は専門整備業者への依頼

第6条(補助記録媒体のセキュリティ管理)

①補助記録媒体の管理責任者は使用者の所属部署長となり、管理責任者は業務用補助記録媒体について別紙第1号書式を使用して管理(登録、破棄、搬出、搬入)しなければならない。登録されていない媒体は使用することができない。

② 重要資料は必ずパスワードが設定されるか、セキュリティプログラムが適用された補助記録媒体に保存する。

③パスワードが設定されるか、又はセキュリティプログラムが適用された補助記録媒体を使用する場合、公認機関等のセキュリティ適合性検証を受けた製品を使用する。

④ 補助記録媒体の紛失時、使用者は直ちに管理責任者に報告する。

⑤ 電算担当部署では、必要に応じて各部署の管理台帳を点検できる。

⑥ 研究員は、補助記録媒体を管理するために管理システムを活用でき、セキュリティ政策及び運営基準は、以下の各号のとおりである。

1. 本システムの目的のために、全職員は会社で使用するパソコンは、補助記録媒体管理のためのクライアントプログラムを設置しなければならない。
2. 会社から流出するすべての資料に対し、同システムを利用して調査できる。
3. 本システムを利用して会社から外部に流出(転送)するすべての資料は、一定期間保管できる。
4. このシステムに登録されていない補助記録媒体の使用は、統制されることができ。

⑦第6項の管理システムを利用して収集した資料は、情報流出の確認作業など会社の情報セキュリティ目的以外のどのような目的であっても公開してはならない。

第7条(個人用コンピュータのセキュリティ管理)

①所属部署長は、会社所有の個人用コンピュータ(デスクトップ、ノートパソコン、一体型、タブレット、その他の形態の情報処理機器を含む。以下、この条において同じ。)の取扱者及びセキュリティ管理責任者を指定しなければならない。

②会社所有の個人用コンピュータで電算ネットワークを使用する職員は、電算部署に登録要請をしなければならない。また、既に使用している個人用コンピュータを交替する場合も同様である。

③ 個人所有の個人用コンピュータを主要情報が処理、保管される研究所の内部に持ち込んで使用することはできない。ただし、やむを得ない場合には、所属部署の長の承認を得て持ち込むことができる。

④会社所有の個人用コンピュータを修理又は交替する場合、情報資料をすべて削除するか、あるいはハードディスクを分離除去した上で修理依頼しなければならない。

⑤個人用コンピュータの使用者は、パスワード設定及びワクチンプログラムをインストール

ールしてセキュリティに万全を期する。

⑥所属部署長は、移動可能な個人用コンピュータ（ノートパソコン、タブレット、一体型等）の搬入・搬出について、別紙第2号書式を利用して管理（登録、移管、搬入、搬出）する。

⑦ 研究員は、全個人用コンピュータの電算セキュリティを強化するために、パッチ管理システムやセキュリティ管理クライアントプログラムを利用でき、業務用のすべての個人用コンピュータはセキュリティ管理クライアントプログラムのインストールを義務づけ、未設置の個人用コンピュータは外部ネットワークの接続を遮断できる。

第8条(電子メール及び通信ネットワークの利用)

①システム管理者(電算部署)は、技術情報セキュリティのために、内部通信ネットワークを利用して内外に受送信する電子メール等により転送される資料については、一定期間(3年以内)内訳を保存しなければならない。

② システム管理者(電算部署)は、職員及び勤務者の業務用Eメール使用のための個人Eメールアカウント(ID)を付与し、職員が退職する場合、直ちにこれを閉鎖しなければならない。ただし、業務協力などの特別な事由がある場合、所属部署長の要請がある場合、3ヵ月の範囲内で閉鎖を留保することができる。

③ システム管理者(電算部署)は迷惑メール、ウイルスメールなどを遮断するために迷惑メール遮断システムを運営する。

④システム管理者(電算部署)は、保存されている資料を情報流出の確認作業など、会社の情報セキュリティ目的以外にいかなる名目であっても公開してはならない。

⑤インターネットの使用は研究員の業務に関するものに限定しなけなければならない、システム管理者(電算部門)は業務に関係のないサイトへのアクセスやプログラムについては使用を制限できる。

⑥ 内部通信ネットワークに接続して個人用コンピュータ等の資料をコピー(ダウンロード)する場合、セキュリティ管理責任者又は所属部署長の承認を受けなければならない。

⑦内部職員は、会社提供の通信ネットワークの使用を原則とし、別途の通信ネットワークの使用が必要な場合は、別紙第3号書式を利用して電算担当部署に申請した上で使用する。

第9条(ホームページ等公開用ウェブサーバーの管理)

①システム管理者は、ホームページ等公開用ウェブサーバーについては、ファイアウォール等侵入遮断システムを設置して、内部ネットワークの電算資源を保護しなければならない。

② システム管理者は、サーバにアクセスできる使用者アカウントを制限し、不必要なアカウントは削除する。

③システム管理者は、ホームページの構築・運営時に独自のセキュリティ検討を経て内容を構成し、その後、個人情報といった重要資料が公開されないようにする。

④システム管理者は、セキュリティ事故に備えて、サーバに保存された資料の徹底したバックアップ体系を構築する。

第10条(無線LANの管理)

- ①無線LANの使用は制限することを原則とする。
- ② 無線通信装置を設置する際、電算担当部署の承認を受けた上で設置し、非認可者の無線LAN接続を防止するため、システム認証及び暗号化等のセキュリティ設定を行う。

第11条(情報セキュリティの責任)

- ①個人が保有している資料等の情報のセキュリティに関する責任は、使用者及び所属部署長にある。
- ②サーバ及び共用情報通信機器に対するセキュリティの責任はシステム管理者にある。
- ③所属部署長は、情報セキュリティ業務の遂行のために、この規定の範囲内で部署の実情に適した別途の対策を設けて施行することができる。

付則

この規定は、代表取締役が承認した日から施行する。

4. 主要契約書の韓国語版

4. 1. 入社者の秘密保持契約書

비밀유지서약서(입사자)

소 속 :

성 명 :

생년월일 : ____년__월__일

위 본인은 20__년__월__일자로 주식회사 ABC(이하 '회사'라 함)에 입사하여, 회사로부터 영업비밀 및 영업자산의 중요성과 영업비밀 등의 보호와 관련한 법령 및 회사의 취업규칙, 영업비밀 관리규정 기타 사규, 방침, 정책 등에 관하여 충분한 설명을 듣고 그 내용을 이해하였기에, 다음 사항을 준수할 것을 서약합니다.

1. 본인은, 아래와 같은 정보가 회사의 영업비밀에 해당함을 확인하며, 회사의 취업규칙, 영업비밀 관리규정 기타 사규, 방침, 정책 등을 준수할 것을 서약합니다.

- ① 영업비밀 관리규정 기타 회사의 내부 규정에 기재된 영업비밀 보호대상
- ② 영업비밀임이 표시된 기술자료, 공장 배치도, 제품 설계도면, 금형, 시제품, 제조 및 판매 매뉴얼, 제조원가, 판매 및 가격결정, 거래선 자료, 인력정보 등에 관한 정보 등
- ③ 통제구역, 시건장치, 패스워드 등으로 접근이 제한된 컴퓨터시스템, 보관함, 통제구역에 보관된 기록매체, 문서, 물건, 정보 등
- ④ [추가 사항 기재]
- ⑤ 그 밖에 회사가 영업비밀로 지정하고 표시하였거나, 회사가 영업비밀로 관리하고 있는 비밀정보

2. 본인은, 회사에 재직 중 취득하게 되는 회사의 영업비밀, 회사의 연구개발·영업·재산 등에 영향을 미칠 수 있는 유형·무형의 정보 기타 회사의 주요 영업자산을 재직 시는 물론 퇴사 후에도 이를 비밀로 유지하고, 회사의

사전 서면 동의 없이는 경쟁업체나 제 3 자에게 제공하거나 누설하지 않으며, 부정한 목적으로 공개하거나 사용하지 않을 것을 서약합니다.

3. 본인은, 회사에 재직 중 취득하게 되는 회사의 영업비밀, 회사의 연구개발·영업·재산 등에 영향을 미칠 수 있는 유형·무형의 정보 기타 회사의 주요 영업자산에대한 모든 권리가 회사의 소유임을 인정하고, 이를 회사에 귀속시킬 것을 서약합니다.

4. 본인은, 회사에 재직 중 회사의 승인을 받지 아니하고는 통제구역, 허가 받지 않은 정보, 시설 등에 접근하지 아니하며, 회사의 영업비밀을 복제하거나 사본 등의 형태로 보관하지 아니할 것을 서약 합니다.

5. 본인은, 입사 전 또는 재직 중에 취득한 타인의 영업비밀 등에 해당하는 정보를 회사에 제공하거나 개시하지 않을 것이며, 업무상 그 정보의 개시가 불가피하다고 판단되는 경우에는 사전에 회사와 상의하여 타인의 영업비밀 등을 침해하지 않도록 할 것을 서약합니다.

6. 본인은, 회사에 재직 중에 회사의 사전 승인을 받지 아니하고는 회사와 동종, 유사업체의 임직원으로 겸직하거나 자문을 제공하지 아니할 것을 서약합니다.

7. 본인은, 회사의 컴퓨터 등 정보처리장치와 정보통신망을 업무용으로만 사용할 것이며, 회사가 불법 행위 방지 및 영업비밀 등의 보호를 위하여 필요한 경우 본인의 컴퓨터 등 정보처리장치나 전자 우편 또는 인터넷 등 정보통신망의 사용 내역, 기타 필요한 정보를 모니터링 할 수 있으며, 불법행위 또는 영업비밀 등의 누설이나 침해의 우려가 있을 경우 관련 내용을 열람할 수 있음을 이해하고, 이에 동의합니다.

8. 본인은, 퇴사 시 재직 중에 보유하였던 회사의 영업비밀, 회사의 연구개발·영업·재산 등에 영향을 미칠 수 있는 유형·무형의 정보 기타 회사의 주요 영업자산과 관련된 자료 모두를 회사에 반납하고, 이에 관한 어떠한 형태의 사본도 개인적으로 보유하지 않으며, 반납할 수 없는 것은 폐기할 것을 서약합니다.

위 서약한 사항을 위반할 경우 관련 법규에 의한 민·형사상 책임을 감수할 것임을
서약합니다.

(위 내용을 확인하고 이해하였으며, 이에 서명함)

20__ . __ . __.

서약자: (서명)

주식회사 ABC 귀하

4. 2. 在職者の秘密保持契約書

비밀유지서약서(재직자)

소속 :

성명 :

생년월일 : ____년 ____월 ____일

본인은 주식회사 ABC(이하 '회사'라 함)에 []년 []월 []일에 입사하여 현재 재직 중인 임직원으로서, 회사로부터 영업비밀 및 영업자산의 중요성과 영업비밀 등의 보호와 관련한 법령 및 회사의 취업규칙, 영업비밀 관리규정 기타 사규, 방침, 정책 등에 관하여 충분한 설명을 듣고 그 내용을 이해하였기에, 다음 사항을 준수할 것을 서약합니다.

1. 본인은, 재직 중 업무 수행 과정에서 취득한 회사의 영업비밀, 회사의 연구개발·영업·재산 등에 영향을 미칠 수 있는 유형·무형의 정보 기타 회사의 주요 영업자산을 비밀로 유지하고, 이와 관련된 법규 및 회사의 취업규칙, 영업비밀 관리규정 기타 사규, 방침, 정책 등을 준수하겠습니다.
2. 본인은, 재직 중 [영업비밀 관련 업무 기재]에 관한 업무를 수행하는 과정에서 취득한 아래 기재와 같은 정보 등이 회사의 영업비밀 혹은 주요 영업자산임을 분명히 인식하고 있습니다.

구분	영업비밀/영업자산의 명칭	영업비밀/영업자산의 설명
1		
2		
3		
4		

3. 본인은, 업무의 수행 중 또는 업무와 관계없이 취득하게 되는 회사의 영업비밀, 회사의 연구개발·영업·재산 등에 영향을 미칠 수 있는 유형·무형의 정보 기타 회사의 영업상 주요 자산을 지정된 업무에 사용하는 경우를

제외하고는 회사의 사전 서면 동의 없이는 어떠한 방법으로도 경쟁업체나 제 3 자에게 제공하거나 누설하지 않으며, 부정한 목적으로 공개하거나 사용하지 않을 것을 서약합니다.

4. 본인은, 재직 중 취득한 회사의 영업비밀, 회사의 연구개발·영업·재산 등에 영향을 미칠 수 있는 유형·무형의 정보 기타 회사의 주요 영업자산에 대한 모든 권리를 회사에 귀속시킬 것을 서약합니다.

5. 본인은, 회사에 재직 중 회사의 승인을 받지 아니하고는 통제구역, 허가 받지 않은 정보, 시설 등에 접근하지 아니하며, 회사의 영업비밀을 복제하거나 사본 등의 형태로 보관하지 아니할 것을 서약합니다.

6. 본인은, 회사에 재직 중에 회사의 사전 승인을 받지 아니하고는 회사와 동종, 유사업체의 임직원으로 겸직하거나 자문을 제공하지 아니할 것을 서약합니다.

7. 본인은, 퇴직 시 회사에 재직 중 보유하였던 회사의 영업비밀, 회사의 연구개발·영업·재산 등에 영향을 미칠 수 있는 유형·무형의 정보 기타 회사의 주요 영업자산 및 이와 관련된 자료 모두를 회사에 반납하고, 이에 관한 어떠한 형태의 사본도 개인적으로 보유하지 않으며, 반납할 수 없는 것은 폐기할 것을 서약합니다.

8. 본인은, 퇴직 시에는 퇴직일로부터 []년의 기간 동안 회사와 합의한 지역 및 직무에 대하여 회사의 영업비밀 혹은 영업자산이 누설되거나 이용될 가능성이 있는 기업, 단체에 취업하거나, 그러 한 기업 또는 단체를 창업 또는 설립하여 경쟁하지 않을 것을 서약합니다. 만약 본인이 취업 혹은 창업하고자 하는 기업 또는 단체가 본 서약서에 따른 경업금지의 대상이 되거나 대상인지 여부가 불분명할 경우, 사전에 회사에 통보하여 회사의 확인 및 동의를 받을 것을 서약합니다.

위 서약한 사항을 위반할 경우 관련 법규에 의한 민·형사상 책임을 감수할 것을 서약합니다.

(위 내용을 확인하고 이해하였으며, 이에 서명함)

20__ . __ . __.

서약자: 홍 길 동 (서명)

주식회사 ABC 귀하

4. 3. 退職者の秘密保持契約書

비밀유지서약서(퇴사자)

소 속 :

성 명 :

생년월일 : ____년__월__일

본인은 []년 []월 []일자로 주식회사 ABC(이하 '회사'라 함)를 퇴사함에 있어서, 회사의 영업비밀 및 영업자산의 보호를 위하여 다음과 같이 서약합니다.

1. 본인은, []년 []월 []일자로 회사에 입사하여 최종적으로 다음과 같은 업무를 수행하였습니다.

[부서명/직책/직급] _____

[업무내용] _____

2. 본인은, 회사에 재직 중 취득한 아래 기재와 같은 영업비밀 및 영업자산을 포함하여 그 밖에 회사의 영업비밀 및 영업자산이 회사의 소유임을 분명히 인식하고 있으며, 퇴사 후에도 이를 비밀로 유지함은 물론 회사의 사전 서면 동의 없이는 경쟁업체나 제 3 자에게 제공하거나 누설하지 않으며, 부정한 목적으로 사용하지 않을 것을 서약합니다.

구분	영업비밀/영업자산의 명칭	영업비밀/영업자산의 설명
1		
2		
3		
4		

3. 본인은, 회사에서 퇴직한 날로부터 []년의 기간 동안 아래 표에서 정하는 지역 내에서 아래 표에 기재한 업무와 관련하여, 위 제 2 항의 영업비밀 및 영업자산을

포함하여, 그 밖에 회사의 영업비밀 및 영업자산이 누설되거나 이용될 가능성이 있는 기업 또는 단체에 취업하거나, 그와 같은 기업 또는 단체를 창업 또는 설립하여 회사와 경쟁하지 않을 것을 서약합니다. 만약 본인이 취업 혹은 창업하고자 하는 기업 또는 단체가 본 서약서에 따른 경업금지의 대상이 되거나 대상인지 여부가 불분명할 경우, 사전에 회사에 통보하여 회사의 확인 및 동의를 받을 것을 서약합니다.

[경업금지 지역] _____

[경업금지 업무] _____

4. 본인은, 퇴사 시 회사로부터 금 []원을 오로지 위 비밀유지 및 경업금지 약정의 대가로 별도 지급 받았으며, 또한 퇴사 후 []년이 되는 시점 및 []년이 되는 시점에 본 서약서에 따른 의무 준수 사실을 회사에 통지하여, 사실로 확인될 경우 각 금 []원을 지급받기로 약정하였습니다.

5. 본인은, 제 2 항 및 제 3 항에서 정하는 의무를 위반할 경우 그로 인한 손해배상으로서 금 []원을 회사에게 지급하고, 이와 별도로 상기 제 4 항에 의하여 지급받은 금 원 및 이에 대한 지급일로부터 이를 반환하는 날까지의 법정이자를 추가하여 회사에게 반환할 것을 약속합니다.

6. 본인은, 퇴사 시 제 2 항의 영업비밀 및 영업자산을 포함하여 그 밖에 회사의 영업비밀 및 영업자산과 관련된 자료를 첨부 영업비밀 자료 반납 확인서와 같이 반납하였고, 반납할 수 없는 것은 폐기하였으며, 이에 관한 어떠한 형태의 사본도 개인적으로 보유하지 않음을 서약합니다.

7. 본인은, 회사가 본인의 퇴사 후 본인이 재직 중에 사용한 컴퓨터 등 정보처리장치나 전자우편 또는 인터넷 등 정보통신망의 사용내역, 기타 필요한 정보를 조사할 수 있으며, 불법행위 또는 영업비밀 등의 누설이나 침해의 우려가 있을 때에는 관련 내용을 열람할 수 있음을 (이해하고, 이에 동의합니다.)

첨부 : 영업비밀 자료 반납 확인서 1부

(위 내용을 확인하고 이해하였으며, 이에 서명함)

20__ . __ . __

서약자: (서명)

주식회사 ABC 귀하

4. 4. 協力会社との秘密保持契約書

비밀유지서약서(협력업체)

주식회사 XYZ(이하 'XYZ'라 함)는(은) 주식회사 ABC(이하 'ABC'라 함)와(과) 상호 협력관계를 유지함에 있어서, ABC의 영업비밀 및 영업자산의 중요성과 영업비밀 등의 보호와 관련한 법령 및 ABC의 영업비밀 관리규정 기타 사규, 방침, 정책 등에 관하여 충분한 설명을 듣고 그 내용을 이해하였기에, 다음 사항을 준수할 것을 서약합니다.

1. XYZ는(은), ABC와(과)의 (협력관계 근거 계약명칭 등) 계약(이하 '협력계약'이라 함)을 이행하는 과정에서 취득하게 되는 ABC의 영업비밀, ABC의 연구개발·영업·재산 등에 영향을 미칠 수 있는 유형·무형의 정보 기타 회사의 주요 영업자산을 비밀로 유지하고, 이와 관련된 법규, 계약 및 ABC의 영업비밀 관리규정 기타 사규, 방침, 정책 등을 준수할 것을 서약합니다.
2. XYZ는(은), 계약을 이행하는 과정에서 취득하게 되는 ABC의 영업비밀, 회사의 연구개발·영업·재산 등에 영향을 미칠 수 있는 유형·무형의 정보 기타 ABC의 주요 영업자산을 지정된 업무에 사용하는 경우를 제외하고는 ABC의 사전 서면 동의 없이 어떠한 방법으로도 제 3자는 물론이고 ABC의 임직원들에게도 제공하거나 누설하지 않으며, 부정한 목적으로 공개하거나 사용하지 않을 것을 서약합니다.
3. XYZ는(은) ABC로부터 사전에 허가 받지 않은 통제구역이나 정보, 시설 등에는 접근하지 않으며, ABC로부터 편의상 제공받은 전산 ID, 패스워드, 출입증 등은 XYZ만이 사용하며 타인에게 공개하거나 대여, 양도하지 않고 계약이 종료될 때에는 이를 반환할 것을 서약합니다.
4. XYZ는(은) 계약의 이행과정에서 취득하게 되는 ABC의 영업비밀, ABC의 연구개발·영업·재산 등에 영향을 미칠 수 있는 유형·무형의 정보 기타 회사의 주요 영업자산에 대한 모든 권리를 ABC가 소유함을 인정하고, 이를 ABC에 귀속시킬 것을 서약합니다.

5. XYZ 는(은) 계약이 기간만료, 해지, 해제 등 여하한 사유로 종료되는 경우에 XYZ 가 계약의 이행 과정에서 취득한 ABC 의 영업비밀, ABC 의 연구개발·영업·재산 등에 영향을 미칠 수 있는 유형·무형의 정보 기타 ABC 의 주요 영업자산 및 이와 관련된 자료 모두를 ABC 에 반납하고, 이에 관한 어떠한 형태의 사본 또는 복제물도 보유하지 않으며, 반납할 수 없는 것은 폐기할 것을 서약합니다.

6. XYZ 는(은) XYZ 의 임직원에게 대해서도 위에서 정한 사항을 준수하도록 본 서약서에 기재된 취지의 의무를 부과하는 등 필요한 조치를 다할 것을 서약합니다.

XYZ 는(은) 위 서약한 사항을 위반할 경우 계약의 해지, 해제 및 관련 법규에 의한 민·형사상 책임을 감수할 것을 서약합니다.

(위 내용을 확인하고 이해하였으며, 이에 서명함)

20__ . __ . __

서약자: 주식회사 XYZ

(주소) _____

대표이사

(인)

주식회사 ABC 귀하

4. 5. 外部者との秘密保持契約書

비밀유지계약서

주식회사 ABC(이하 'ABC'라 함)와(과) 주식회사 XYZ(이하, 'XYZ'라 함)는(은) 비밀정보의 제공과 관련하여 다음과 같이 비밀유지계약을 체결한다.

다 음

제1조 (계약의 목적)

본 계약은 ABC 와(과) XYZ 가 『 (업무 요지 기재) (이하 '본 업무'라 함)』와 관련하여 각자 상대방에게 제공하는 비밀정보를 비밀로 유지하고 보호하기 위하여 필요한 제반 사항을 규정함을 목적으로 한다.

제2조 (비밀정보의 정의)

- ① 본 계약에서 '비밀정보'라 함은, ABC 또는 XYZ 가 본 업무 수행 과정에서 스스로 알게 되거나, 상대 방 또는 그 직원(이하 '상대방'이라 함)으로부터 제공받아 알게 되는 상대방에 관한 일체의 기술상 혹은 경영상의 정보 및 이를 기초로 새롭게 발생한 일체의 기술상 혹은 경영상의 정보를 말한다.
- ② 제 1 항의 비밀정보는 서면(전자문서를 포함하며, 이하 같음), 구두 혹은 기타 방법으로 제공되는 모든 노하우, 공정, 도면, 설계, 실험결과, 샘플, 사양, 데이터, 공식, 제법, 프로그램, 가격표, 거래명세서, 생산단가, 아이디어 등 모든 기술상 혹은 경영상의 정보와 그러한 정보가 수록된 물건 또는 장비 등을 모두 포함한다.

제3조 (비밀의 표시)

- ① 각 당사자가 상대방에게 서면으로 비밀정보를 제공하는 경우, 그 서면에 비밀임을 알리는 문구('비밀' 또는 '대외비' 등의 국문 또는 영문 표시)를 표시해야 한다.
- ② 각 당사자가 상대방에게 구두나 영상 또는 당사자의 시설, 장비 샘플 기타 품목들을 관찰·조사하게 하는 방법으로 비밀정보를 제공할 경우에는, 그 즉시 상대방에게 해당 정보가 비밀정보에 속한다는 사실을 고지하여야 한다. 이때 비밀정보를 제공한 당사자는 비밀정보 제공일로부터 15 일 이내에 상대방에게 해당 정보가 비밀정보에 속한다는 취지의 서면을 발송하여야 한다.

제4조 (정보의 사용용도 및 정보취급자 제한)

- ① 각 당사자는 상대방의 비밀정보를 '본 업무'의 수행 또는 '본 업무'와 관련된 계약에서 정한 본래의 목적으로만 사용하여야 한다.
- ② 각 당사자가 '본 업무'의 수행을 위하여 상대방의 비밀정보를 제 3 자에게 제공하고자 할 때에는 사전에 상대방으로부터 서면에 의한 동의를 얻어야 하며, 그 제 3 자와 사이에 해당 비밀정보의 유지 및 보호를 목적으로 하는 별도의 비밀유지계약을 체결한 이후에 그 제 3 자에게 해당 비밀정보를 제공하여야 한다.
- ③ 각 당사자는 직접적, 간접적으로 '본 업무'를 수행하는 임직원들에 한하여 상대방의 비밀정보를 취급할 수 있도록 필요한 조치를 취하여야 하며, 해당 임직원 각자에게 상대방의 비밀정보에 대한 비밀유지의무를 주지시켜야 한다. 이때 상대방은 반대 당사자에게 해당 임직원으로부터 비밀유지 서약서를 제출 받는 등의 방법으로 해당 정보의 비밀성을 유지하기 위하여 필요한 조치를 요구할 수 있다.

제5조 (비밀유지의무)

- ① 각 당사자는 상대방의 사전 서면승낙 없이 비밀정보를 포함하여 본 계약의 체결사실이나 내용, '본 업무'의 내용 등을 공표하거나 제 3 자에게 알려서는 아니 된다. 다만, 객관적인 증거를 통하여 다음 각 호에 해당함이 입증되는 정보는 비밀정보가 아니거나 비밀유지의무가 없는 것으로 간주한다.
 1. 상대방의 비밀정보 제공 이전에 다른 당사자가 이미 알고 있거나 알 수 있는 정보
 2. 비밀정보를 제공받은 당사자의 고의 또는 과실에 의하지 않고 공지의 사실로 된 정보
 3. 비밀정보를 제공받은 당사자가 적법하게 제 3 자로부터 제공받은 정보
 4. 비밀정보를 제공받은 당사자가 비밀정보와 관계없이 독자적으로 개발하거나 알게 된 정보
 5. 제 3 조 제 2 항에 의하여 비밀정보임을 고지하지 아니하거나, 비밀정보에 속한다는 취지의 서면을 발송하지 아니한 정보
 6. 법원 기타 공공기관의 판결, 명령 또는 관련법령에 따른 공개의무에 따라서 공개한 정보
- ② 각 당사자가 제 1 항 제 6 호에 따라 정보를 공개할 경우에는 사전에 상대방에게 그 사실을 서면으로 통지하고, 상대방으로 하여금 적절한 보호 및 대응조치를 할 수 있도록 하여야 한다.

제6조 (자료의 반환)

- ① 각 당사자는 상대방의 요청이 있으면 언제든지 상대방의 비밀 정보가 기재되어 있거나 이를 포함 하고 있는 제반 자료, 장비, 서류, 샘플, 기타 유체물(복사본, 복사물, 모방물건, 모방장비 등을 포함)을 즉시 상대방에게 반환하거나, 상대방의 선택에 따라 이를 폐기하고 그 폐기를 증명하는 서류를 상대방에게 제공하여야 한다.

- ② 제 1 항의 자료의 반환 또는 폐기에 소요되는 비용은 각 당사자가 균등하게 부담하기로 한다. 다만, 자료의 반환 또는 폐기 의무자가 우선 그 비용을 지출한 이후 상대방에게 그 부담부분을 정산하여 청구하기로 한다.

제7조 (권리의 부존재 등)

- ① 본 계약에 따라 제공되는 비밀정보에 관한 모든 권리는 이를 제공한 당사자에 속한다.
- ② 본 계약은 어떠한 경우에도 비밀정보를 제공받는 자에게 비밀정보에 관한 어떠한 권리나 사용권을 부여하는 것으로 해석되지 않는다.
- ③ 본 계약은 어떠한 경우에도 당사자 간에 향후 어떠한 확정적인 계약의 체결, 제조물의 판매나 구입, 실시권의 허락 등을 암시하거나 이를 강제하지 않으며, 기타 본 계약의 당사자가 비밀정보와 관련하여 다른 제 3 자와 어떠한 거래나 계약관계에 들어가는 것을 금지하거나 제한하지 아니한다.
- ④ 비밀정보의 제공자는 상대방에게 비밀정보를 제공할 적법한 자격이 있음을 보증한다.
- ⑤ 각 당사자는 본 계약의 목적을 위하여 상대방의 시설을 방문하거나 이를 이용할 경우에는 상대방 의 제반 규정 및 지시사항을 준수하여야 한다.

제8조 (계약기간)

- ① 본 계약은 본 계약 체결일로부터 []년간 그 효력을 가진다.
- ② 제 1 항에도 불구하고, 본 계약 제 4 조, 제 5 조 및 제 7 조의 의무는 본 계약의 계약기간이 만료되거나, 본 계약이 해제·해지 등의 사유로 종료된 이후부터 계속하여 유효하게 존속하는 것으로 한다.

제9조 (손해배상, 위약벌)

- ① 본 계약을 위반한 당사자는 이로 인하여 상대방이 입은 모든 손해를 배상하여야 한다.
- ② 본 계약을 위반한 당사자는 제 1 항의 손해배상과 별도로 상대방에게 위약벌로서 금 []원 을 지급하여야 한다.

제10조 (권리의무의 양도, 계약의 변경)

- ① 각 당사자는 상대방의 사전 서면동의 없이 본 계약상의 권리의무를 제 3 자에게 양도하거나 이전할 수 없다.
- ② 본 계약의 수정이나 변경은 양 당사자의 정당한 대표자가 기명날인 또는 서명한 서면합의로만 이루어질 수 있다.

제11조 (계약의 분리가능성)

본 계약 중 어느 규정이 법원에 의하여 위법, 무효 또는 집행 불가능 하다고 선언될 경우에도, 이는 본 계약의 나머지 규정의 유효성에 영향을 미치지 아니한다.

제12조 (분쟁의 해결)

본 계약과 관련하여 분쟁이 발생한 경우 당사자의 상호 협의에 의한 해결을 모색하되, 분쟁에 관한 합의가 이루어지지 아니한 경우에는 [서울중앙지방법원]을 제 1 심 관할법원으로 하여 소송을 통해 분쟁을 해결하기로 한다.

‘ABC’와(과) ‘XYZ’는(은) 본 계약의 성립을 증명하기 위하여 본 계약서 2 부를 작성하여 각각 서명(또는 기명날인)한 후 각자 1부씩 보관한다.

20__년 __월 __일

“ABC”

(명칭)_____

(주소)_____

(대표자)_____ (인)

“XYZ”

(명칭)_____

(주소)_____

(대표자)_____ (인)

〔経済産業省委託事業〕
韓国における営業秘密管理マニュアル

2022年2月発行
禁無断転載

〔調査受託〕
韓洋国際特許法人(代表弁理士 金延洙)

〔著者〕
韓洋国際特許法人(代表弁理士 金延洙)
金世元 パートナー弁理士
姜錫勳 弁理士
鄭熙景 国際部
草野達也 国際部

〔オブザーバー〕
日本貿易振興機構 ソウル事務所
土谷慎吾
柳忠鉉

本冊子は、作成時点に入手した情報に基づくものであり、その後の状況によって変わる場合があります。また、掲載した情報・コメントは著者及び当機構の判断によるものですが、一般的な情報・解釈がこのとおりであることを保証するものでないことを予めお断りします。

経済産業省委託事業

営業秘密に関する欧米の法制度調査

2022 年 3 月

独立行政法人 日本貿易振興機構
ニューヨーク事務所

目次

はじめに.....	6
米国.....	8
第1章 営業秘密の定義.....	8
1 判例法/UTSA/DTSA による定義.....	9
2 秘密性保護の措置.....	10
3 州法の定義の DTSA による影響.....	11
第2章 営業秘密侵害行為の定義.....	11
1 判例法における営業秘密侵害行為.....	111
2 DTSA における営業秘密侵害行為.....	13
3 ミスによる営業秘密の取得.....	13
4 主観的要件と救済.....	14
5 除外規定.....	14
6 恒久的差止命令等の救済措置における利益調整.....	16
7 損害賠償における利益調整.....	16
8 時効.....	17
第3章 営業秘密侵害に関連する法律、規制の概要(判例法/UTSA/DTSA 以外).....	17
1 1930 年関税法.....	17
2 連邦経済スパイ法.....	18
3 州刑事法.....	20
4 秘密保持条項違反.....	21
5 通信関連機器に関する刑事法.....	22
6 営業秘密事件の審理と措置.....	23
7 損害賠償.....	28
第4章 営業秘密事件の実務.....	28
1 保護される営業秘密.....	28
2 営業秘密侵害行為の認定.....	29
3 訴訟提起及び証拠収集段階における営業秘密の保護.....	31
4 救済手段、営業秘密保護の現状.....	32
5 内部告発と営業秘密の使用・開示.....	34
第5章 準拠法・域外適用.....	34

1 判例法での準拠法	34
2 侵害品の輸入と米国関税法の適用	35
3 DTSA 下の侵害行為と域外適用	35
第6章 営業秘密侵害の事件数	36
1 訴訟数の概観	36
2 訴訟結果	36
3 解決の期間	37
4 連邦経済スパイ法	37
第7章 営業秘密関連の法改正の動き	38
1 営業秘密法	38
2 サイバーセキュリティ政策	38
第8章 国際協力・他国との連携状況	40
第9章 仲裁の利用	42
第10章 ライセンス、生産委託、合弁会社設立で気をつけるべきポイント	42
1 ライセンス契約	43
2 生産委託契約	44
3 合弁契約	45
欧州	46
第1章 営業秘密の定義	46
1 EU 指令の制定と主要加盟国の国内法移行	46
2 EU 指令による「営業秘密」の定義	46
第2章 営業秘密侵害行為の定義	48
1 EU 指令における営業秘密侵害行為	48
2 営業秘密侵害行為に対する例外	50
第3章 営業秘密侵害に関連する法律、規制の概要	50
1 EU 指令の国内法移行	50
2 営業秘密侵害に対する刑事処罰	52
第4章 営業秘密事件の実務	54
1 民事的救済措置の付与義務と救済措置の内容（EU 指令第3章第1節）	54
2 暫定的措置及び予防的措置（EU 指令第3章第2節）	56
3 本案判断から生じる措置（EU 指令第3章第3節）	57

4 行政措置.....	59
第5章 域外適用.....	61
第6章 営業秘密侵害の事件数.....	61
第7章 営業秘密関連の法改正.....	62
1 営業秘密法.....	62
2 デジタル化競争政策.....	62
3 デジタルサービス適正化.....	68
第8章 国際協力・他国との連携状況.....	71
第9章 仲裁の利用.....	73
第10章 ライセンス、生産委託、合弁会社設立で気をつけるべきポイント.....	73
1 ライセンス契約.....	74
2 生産委託契約.....	76
3 合弁契約.....	76
ドイツ.....	77
第1章 営業秘密の定義.....	77
1 判例法による定義.....	77
2 GeschGehG による定義.....	78
第2章 営業秘密侵害行為の定義.....	80
1 従前の判例法における営業秘密侵害行為.....	80
2 新法における営業秘密侵害行為.....	80
3 新法と判例法の差異.....	81
第3章 営業秘密侵害に関連する法律、規制の概要.....	82
1 GeschGehG.....	82
2 刑法.....	84
3 民法.....	84
4 商法.....	85
5 その他関連法改正.....	85
第4章 営業秘密事件の実務.....	86
1 知的財産権訴訟の訴訟提起および証拠収集段階における営業秘密の保護.....	86
2 救済手段、営業秘密保護の現状.....	87
3 公務員による秘密の不正流用.....	89

4 内部告発と営業秘密の使用・開示	89
第5章 準拠法・域外適用	90
第6章 営業秘密侵害の事件数	90
第7章 営業秘密関連の法改正の動き	91
1 営業秘密法	91
2 デジタル化政策	91
3 サイバーセキュリティ政策	91
4 5G 環境の整備	92
第8章 国際協力・他国との連携状況	94
第9章 仲裁の利用	95
第10章 ライセンス、生産委託、合併会社設立で気をつけるべきポイント	95
1 ライセンス契約	96
2 生産委託契約	97
3 合併契約	98
英国	99
第1章 営業秘密の定義	99
1 新法による定義	99
2 判例法による定義	99
3 新法と判例法の差異	100
第2章 営業秘密侵害行為	101
1 新法による営業秘密侵害行為の定義：営業秘密不正取得・開示・使用	101
2 判例法による守秘義務違反の原理：機密情報の不正取得・開示・使用	102
3 新法と判例法の差異	105
第3章 営業秘密侵害に関連する法律、規制の概要	106
1 営業秘密侵害行為に関する EU 指令及び UK TS 規則	106
2 契約関係を基礎とする守秘義務違反	109
3 衡平法下における守秘義務違反	110
4 コンピューター不正使用法	110
5 競争法	112
6 刑事営業秘密法	113
7 重複する知的財産権侵害に基づく請求	113

第4章 営業秘密、機密情報事件の実務（本案裁判例、付随する措置）	114
1 EU指令/UK TS規則による営業秘密保護とコモンローの機密情報保護との関係を問題とした判例	114
2 EU指令/UK TS規則による営業秘密保護とコモンローの機密情報保護と両者を取り扱った判例	114
3 機密情報保護の暫定的措置の期間設定、賠償額算定の基礎	115
4 秘密保持契約の効力を否定した例	116
5 暫定措置の内容を複数の期間に分割して、異なった内容の秘密保持措置を命じ、擬制信託を否定し、秘密保有者の「汚い手」について言及した例	116
6 暫定的措置	117
第5章 域外適用	119
第6章 営業秘密、機密情報の事件数（本案裁判例）	120
1 刑事	120
2 民事	120
第7章 営業秘密関連の法改正	121
第8章 国際協力・他国との連携状況	121
第9章 仲裁の利用	122
第10章 ライセンス、生産委託、合弁会社設立で気をつけるべきポイント	122
1 ライセンス契約	123
2 生産委託契約	124
3 合弁契約	125
参考書式 目次	126

はじめに

我が国が先進国に数えられるようになって以来、営業秘密は、経済社会で活動を行っている個人、法人の重要な資産であり続けている。高機能の製品やサービスを生み出すためには、これからも、あるいは、これまで以上に、営業秘密の創出、管理、及び、保護が欠かせないことは、疑問の余地がない。

医薬品、無人乗用車、無線通信、AI 関連発明など、競争の激しい産業分野では、技術の安定で確実な製品化、そのスピードが勝敗を決することが多い。従って、これらの分野で事業を行う者には、特に、営業秘密の管理が企業の存続と発展に不可欠となってきた。こうした状況は、Innovator 企業の営業秘密をターゲットとする、国際産業スパイによる盗取、詐取事件の報道や、技術開発部門担当者や営業部社員からライバル企業への漏洩事件の発覚が増えるにつれて、適切な対応が急がれる事項の一つとなり、深刻な問題として認識されるようになってきた。

また、センサーの高性能化、情報通信の加速化、ネットワークの万能化は、ありとあらゆる事象を、データとして捉えることを可能にし、営業秘密は、数、価値ともに増えていくものと考えられる。これに加え、巨大な情報のクラウド保存により、厳密な情報管理は、費用的に困難なこともわかっており、営業秘密の保護に、これまでになかった挑戦を与えている。さらに、新型コロナウイルスの世界的拡大とそれに伴うリモートワークの普及により企業外部での就業機会が世界的に拡大する中で、サイバー攻撃は大幅に増え、企業の技術的弱点につけこむ手口も巧妙化しつつある。

他方で、巨大データの蓄積、技術標準化等を通じて、限られた企業が複数のマーケットで支配的地位を獲得している状況は問題視されている。更に、構造的不況の持続、及び、必要とされる技術力の変化から、雇用の不安定化や被用者の雇用を求める権利保護が課題となっている。営業秘密の適切かつ実効的に保護するための仕組みの確立と、技術情報や雇用機会への平等なアクセス、透明性の確保も無視できないと考えられる。

以上のような状況は、諸外国でも同様にみられている。米国では、州レベルでは、1971 年に発表された「統一営業秘密法」あるいは（及び）「不法行為法リステートメント」に基づき、保護が付与されていたところであるが、連邦レベルでも、1996 年施行された「産業スパイ法」、さらに、2016 年に制定された「営業秘密保護法」を活用して、営業秘密の保護が可能となっている。共和党のトランプ前大統領は、中国政府、中国企業による知的財産権や国家機密の不正取得を厳しく摘発し、訴追を行っているが、その傾向は、民主党に政権が移行しても継続している。

ヨーロッパ全域での営業秘密保護の主要な歩みとして、ヨーロッパ連合で、2017 年に、各

加盟国での制度整備を求める「営業秘密指令」が成立した。これを受け、各国で法改正がなされ、上記の問題に対応すべき措置も幾つか明文で講じられた。英国は、EU を脱退したが、脱退前に、前述の指令に基づいた営業秘密法が誕生しており、従前のコモンローに基づく保護が補強された。

こうした状況を踏まえ、本事業では、米国、英国、EU、及びドイツにおける、営業秘密保護の実態や動向を調査し、立法、司法制度の状況を調査し、米国、英国、EU、及びドイツにおける、情報管理体制を整備する方法、規程や契約、具体的な管理体制・枠組み(営業秘密の保護)のあり方を検討するためのマニュアルを作成した。

本マニュアルが、米国、英国、EU、及びドイツで事業を行う日系企業の営業秘密保護のために、何らか役立つものとなれば幸いである。

米国

第1章 営業秘密の定義

米国は、英国と同様にコモンローの国であるところ、営業秘密の保護は、民事法体系では、判例法に基づく不法行為法、不正競争防止法が主に関連しており、長年にわたり発達してきた¹。1979年に、統一法委員会（ULC）がモデルの営業秘密法（UTSA）を作成し、現在までに、ニューヨーク州を除く全州が UTSA を採用し、営業秘密保護法を立法化して保護を与えている²。

また、米国刑事法では、州レベルで、長年に亘って窃盗罪等（対象となる無体物に含める、あるいは営業秘密を条文に明記する）として処罰されてきたところ、UTSA 作成後に、UTSA に沿った内容に改正されるなどされている。さらに、1996年の連邦経済スパイ法により、営業秘密侵害を連邦法上の重犯罪として扱うことができるようになった。

さらに、2016年、連邦法として営業秘密保護法（DTSA）が制定されて以降、営業秘密保有者は、営業秘密侵害の事実に関して、州の裁判所だけでなく、連邦裁判所においても、民事上の法的救済を求められるようになった³。DTSA は、連邦裁判所での救済の付与以外にも、(1) 営業秘密法の統一、(2) 外国人、外国法人による営業秘密侵害に対する救済の実効化、(3) 一方的証拠品押収手続 (ex parte seizure) による立証方法の容易化を目指していた。DTSA のこれらの立法目的のうち、連邦裁判所へのアクセスを与えるという目的、(2) 外国人、外国法人による侵害への救済付与との目的は、同法施行により実現されているとされるが、(1) 営業秘密法の統一、(3) 一方的証拠品押収手続の点については、実現あるいは利用が進んでいないとの見方が強い⁴。

1 判例法/UTSA/DTSA による定義

(1) 判例法による定義

¹ 契約上の義務不履行を除く請求、即ち、不法行為、不当利得、守秘義務違背、営業秘密の窃取といった契約に基づかない請求は、営業秘密侵害に関するコモンローの判例法が適用になるとされる。Restatement (First) of Torts, § 757, cmt. b (1939)、Restatement (Third) of Unfair Competition, §§ 39, 40 cmt. a (1995)、Penalty Kick Management Ltd. v, Coca Cola Co. 318 F.3d 1284 (2003)。

² 営業秘密、法律情報所 (最終アクセス日 2022 年 2 月 18 日), https://www.law.cornell.edu/wex/trade_secret.

³ 法律情報所、脚注 2

⁴ Mark Klapow, et al. How 5-Year-Old Trade Secrets Act Has Met Its Goals, Law360 (2021).

従前の判例に基づく定義によると、情報のうち、下記の要素を考慮して、営業秘密として認めるべきものを言う判断されており、実体が掴みづらい定義となっていた⁵。

- a. 保有者の事業以外で、情報が知られている程度
- b. 事業に携わる従業員や、その他の人々に、どの程度知られているか
- c. 情報の秘密を守るために、保有者が講じた措置の程度
- d. 保有者の事業と、その競合他社にとっての、情報の価値
- e. 情報を開発するために企業が費やした労力又は金銭の量
- f. 情報が、他者によって、適切に取得、若しくは、複製される可能性の容易さ、又は、困難さ

(2) UTSA による定義

UTSA は、下記のように営業秘密を定義しており、TRIPS 協定第 39 条第 2 項の開示されていない情報（営業秘密）の定義と合致したものとなっている⁶。

製法（方式）、パターン、集積、プログラム、装置、方法、技術、又はプロセスを含む、次のような情報。

- a. その開示、又は、使用から、経済的価値を得られる他者により、一般的に知られていない、かつ、適法な手段によって容易に確認できないことから、実際の、又は、潜在的な、独立した経済的価値を導き出す
- b. その秘密性を維持するため、当該状況下で、合理的な努力の対象となっている

(3) DTSA による定義

DTSA は、営業秘密を、下記のように定義する⁷。

秘密性を維持するために合理的な措置が取られていた情報で、その開示、又は、使用から経済的価値を得られる他者に一般に知られておらず、かつ、適法な手段により容易に知ることができないことから、独立した経済的価値を導き出すもの

この定義は、UTSA の定義とほぼ同様であり、UTSA を採用した州法の営業秘密の定義と概ね同様であると理解されている⁸。

⁵ Restatement (First) of Torts、脚注 1

⁶ 1985 年の改変を含んだ統一営業秘密法、統一州法委員全国会議（1985）（「UTSA」）
<https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=e19b2528-e0b1-0054-23c4-8069701a4b62>.

⁷ 18 U.S.C. § 1839(3).

⁸ Klapow、脚注 4 参照。

2 秘密性保護の措置

D TSA における「合理的な秘密性保持の措置」及び UTSA における「秘密性維持のための合理的な努力の対象」に関して、各裁判所の解釈は相当分かれているとの見解が強い⁹。裁判所において、下記のように、営業秘密に対する保護措置が取られていない可能性があると判断する、あるいは示唆することがある。

- a. 秘密保持義務を課さずに、顧客あるいは顧客となりうる者に情報をシェアしたこと¹⁰
- b. 従業員に、会社業務専用の携帯、コンピューター等、通信・処理装置を与えていなかったこと（又は、私用の携帯の使用を許可した）¹¹
- c. 機密情報の定義が限定的で、範囲が狭すぎたこと¹²
- d. 秘密保護義務を課す契約前に情報を開示したこと¹³
- e. 明示的に「機密情報」と告げる等、指定をしなかったこと¹⁴
- f. 「機密情報」とのラベルの欠如¹⁵
- g. 従業員の秘密保護義務への署名拒否の事実¹⁶

したがって、裁判所は、次のような事実の有無を重要視することは、明らかである。

- i. 情報は、割り当てられた仕事を実行するため、少なくとも潜在的にアクセスを必要とする人にものみ開示されている（「知る必要があるベース」）、
- ii. 情報が開示される人は、秘密保持義務に拘束され、情報に関して、この秘密保持義務を負っていることを認識している。

特に、裁判所は、一定の機密性保持の努力に関して（従業員が、会社から貸与されたハードウェアではなく、自分のハードウェアにファイルを保存することを阻止しなかったこと等）、同種の業界で、機密情報の保護に必要な場合に、通常取られている措置がとられていないことは、「合理的な秘密性保護の措置が存在した」事実を否定する、一種の抗弁となる

⁹ Joseph W. Hammell, Protection of Employers' Trade Secrets and Confidential Information, Practical Law Practice Note 5-501-1473 (Westlaw 2021)

¹⁰ Yellowfin Yachts, Inc. v. Barker Boatworks, LLC, 898 F.3d 1279, 1299-1301 (11th Cir. 2018)、Madison Oslin v. Interstate Res., No. MJG-12-3041, 2015 U.S. Dist. LEXIS 37587 (D. Md. Mar. 25, 2015)、Prostar Wireless Group v. Domino's Pizza, 360 F. Supp. 3d 994 (N.D. Cal. 2018)

¹¹ Encompass Services, PLLC v. Maser Consulting, P.A. and Hilsman, 2019 NCBC 66 (J. McGuire).

¹² 機密情報として、ソフトウェアのソースコード、その構造、アルゴリズムとのみ指定していた。Broker Genius v. Zalta, 280 F. Supp. 3d 495 (S.D.N.Y. 2017)

¹³ Smart & Assocs. v. Indep. Liquor (NZ) Ltd., 226 F. Supp. 3d 828 (W.D. Ky. 2016)

¹⁴ Big Vision Private v. E.I. Dupont De Nemours & Co., 1 F. Supp. 3d 224 (S.D.N.Y. 2014)

¹⁵ Yellowfin Yachts, Inc. v. Barker Boatworks, LLC, 898 F.3d 1279, 1299-1301 (11th Cir. 2018)

¹⁶ Yellowfin Yachts, Inc. v. Barker Boatworks, LLC, 898 F.3d 1279, 1299-1301 (11th Cir. 2018)

と考えているようにも解釈できる。

3 州法の定義の DTSA による影響

州法による営業秘密の定義は若干差異があるため、ある州で営業秘密として認められたとしても、別の州が反対の結論に達する可能性があり、こうした状況は DTSA 制定によっても変わっていないと理解されている¹⁷。

ただし、以下のような情報は、大体の州で、営業秘密として保護されている。

- マーケティング計画
- 商業図面
- 食品等のレシピ
- 販売データ
- 製造プロセス
- 化学式
- 顧客に関する、詳細情報。

後述の第 4 章「営業秘密事件の実務」で、DTSA 制定後、DTSA の営業秘密の定義等についての裁判例を紹介し、むしろ、州法の定義が DTSA に影響を与えるという、本来の立法目的と逆の現象が見られていることに言及する。

第 2 章 営業秘密侵害行為の定義

1 判例法における営業秘密侵害行為

従来より、コモンローの下で、請求の基礎として営業秘密の侵害行為、すなわち、不正な使用・開示、又は違法な取得がされたことが、必要であった¹⁸。具体的に、違法な取得、又は、不正な使用・開示を構成する行為は、不正な方法でなされるか、若しくは、守秘義務に違反してなされる場合とされてきた¹⁹。

(1) UTSA (州法) による営業秘密侵害行為

UTSA において、つまり殆どの州では、下記の行為が違法な侵害行為とされている²⁰。

¹⁷ Farmers' Edge Inc. v. Farmobile, LLC, 970 F.3d 1027, 1033 (8th Cir. 2020)

¹⁸ 法律情報所、脚注 2

¹⁹ Restatement (First) of Torts, § 757(1939)、Restatement (Third) of Unfair Competition, § 39 (1995)

²⁰ UTSA 第 1 条 オハイオ州の営業秘密法は、UTSA をほぼそのまま制定法化したものである。Allied Erecting & Dismantling Co. v. Genesis Equip. & Mfg., Inc., 649 F. Supp. 2d 702, 711–12 (N.D. Ohio 2009)

- a. 他人の営業秘密が、不正な方法で取得されたことを認識しているか、認識すべきであった者による、当該営業秘密の取得。
- b. 以下の者による、明示、若しくは、黙示の同意なき、他人の営業秘密の開示、又は、使用。
 - i. 当該営業秘密を不正な方法を用いて取得
 - ii. 開示、若しくは、使用のときに、自己の営業秘密に関する知識が、
 - a) 営業秘密を不正な方法を用いて取得した者に由来して、又は、その者を介して得られた、
 - b) 秘密性を保持すべき、あるいは、使用を制限すべき義務を負うと考えられる状況で得られた、又は、
 - c) 救済請求者に、秘密性を保持すべき、あるいは、使用を制限すべき義務を負っていた者に由来して、又は、その者を介して得られた、
ことを認識していたか、認識すべきであった。
 - iii. 重大な状況の変化が生じる前に、得た知識が、他人の営業秘密で、偶然、あるいは、ミスで得られたことを認識していたか、認識すべきであった。

(2) 第三者の行為

判例法、UTSA にならって制定された州法のもとでも、契約関係に立つ者以外の者が、故意もしくは過失により、営業秘密の不正な開示、取得、使用をした場合においても、民事的救済を受けることが可能であった²¹。例えば、不正に取得された営業秘密を使用している製品やサービスを作成、販売、輸出入、市場に提供する者の行為を対象として、民事的救済措置（金銭的損害賠償を含む）を求めることができていた²²。

例えば、製造委託の注文に際し、他人によって営業秘密侵害との訴えを起こされているにもかかわらず、不正に取得した営業秘密を、受託者たる製造者に対して提供し、営業秘密保有者からのライセンスがある旨、信用性に乏しい説明をしていた場合、受託者が、そのような説明を鵜呑みにするのは、事情を「認識すべきであった」ので、侵害にあたるとされる

²³。

²¹ UTSA や各州法の定義では、不正な取得、不正な開示、又は、使用とは、その状況下で、営業秘密が、不正に取得等された事実を知っていたか、知るべきであった場合には、営業秘密の侵害となるとされている。UTSA 第 1 条

²² Restatement (First) of Torts, § 757(1939)、Restatement (Third) of Unfair Competition, § 39 (1995)、UTSA 第 1 条

²³ Cognis Corp. v. CHEMCENTRAL Corp., 430 F. Supp. 2d 806, 812–13 (N.D. Ill. 2006)

2 DTSA における営業秘密侵害行為

(1) DTSA の侵害行為の定義²⁴

DTSA は、UTSA をほぼ踏襲して、営業秘密侵害行為を次のように定めている。

- a. 他人の営業秘密が、不正な方法で取得されたことを認識しているか、認識すべきであった者による、当該営業秘密の取得
- b. 以下に該当する、明示、若しくは、黙示の同意の無い、他人の営業秘密の開示、又は、使用：
 - i. 当該営業秘密を不正な方法を用いて取得
 - ii. 開示、若しくは、使用のときに、自己の知識が、
 - a) 営業秘密を不正な方法を用いて取得した者に由来して、又は、その者を介して得られた、
 - b) 秘密性を保持すべき、あるいは、使用を制限すべき義務を負うと考えられる状況で得られた、又は、
 - c) 救済請求者に、秘密性を保持すべき、あるいは、使用を制限すべき義務を負っていた者に由来して、又は、その者を介して得られた、ことを認識していたか、認識すべきであった
 - iii. 重大な状況の変化が生じる前に、得た知識が、他人の営業秘密で、偶然、あるいは、ミスで得られたことを認識していたか、認識すべきであった。

(2) 第三者の行為²⁵

DTSA も、UTSA、即ち、判例法と同様、契約関係に立つ者以外の者が、過失により営業秘密の不正な開示、取得、使用をした場合においても、民事的救済を受けることが可能であるとする。例えば、不正に取得された営業秘密を使用している製品やサービスを作出、販売、輸出入、市場に提供する者の行為を対象として、民事的救済措置(金銭的損害賠償を含む)を求めることができる²⁶。

3 ミスによる営業秘密の取得

上記の通り、判例法上も、DTSA でも、重大な状況の変化が生じる前に、営業秘密であると

²⁴ 18 U.S.C. § 1839(5)

²⁵ UTSA や各州法の定義では、不正な取得、不正な開示、又は、使用とは、その状況下で、営業秘密が、不正に取得等された事実を知っていたか、知るべきであった場合には、営業秘密の侵害となるとされている。

²⁶ 18 U.S.C. § 1839(5)

認識できた者が（従前から取引していた同業者や内部関係者等）、たまたま情報を受け取ってしまった場合（Eメールを誤って送られた場合等）、その情報を勝手に開示したり、使用したりした場合には、営業秘密侵害行為となる²⁷。すなわち、営業秘密保有者によるそのようなミスにもかかわらず、「秘密性保持の合理的措置」に欠けると判断されず、営業秘密は保護されたままである。もちろん、そのミスの後の是正措置が秘密性の保護手段として相当であったかが争点となる。

4 主観的要件と救済

UTSA 第 1 条、DTSA 定義規定によると、不正な使用又は開示にあたるのは、行為者が、所定の事情の存在下に²⁸、自分が「営業秘密の知識を」得たことを認識していたか、認識すべきであった場合である²⁹。これを、文言通りに解釈すると、所定の事情について、故意あるいは過失を有していたことが必要で、かつ、「営業秘密」についての知識（ないしは認識）が、必要であるかのようにも読める。しかし、裁判例は、これを広義に解し、営業秘密の具体的内容を直接に知っていないような第三者にも、自分の情報元が、当該情報について守秘義務を負っているような状況、あるいは、侵害にあたりうる行為により取得したことを、知っているか、知るべきであった事実があれば、「営業秘密の知識を」得たと認定している³⁰。

その他、主観的要件が救済内容に影響を与えることは、後述のとおりである³¹。

5 除外規定

(1) 判例法

判例法では、以下の場合には、「不正」取得、開示、使用にはあたらないと解されてきた³²。

- 保有者と独立して営業秘密を取得した場合
- 既に適正に知られていた情報・物件を、リバースエンジニアリングして取得し

²⁷ UTSA 第 1 条、18 U.S.C. § 1839(5).

²⁸ 所定の事情とは、UTSA では、(i)営業秘密を不正な方法を用いて取得した者に由来して、又は、その者を介して、(ii)秘密性保持、あるいは、使用制限の義務を負う状況において、又は、(iii)救済を求める者に、秘密性保持、あるいは、使用制限義務を負っていた者に由来して、又は、その者を介して、

²⁹ UTSA 第 2 条、18 U.S.C. § 1839(5)

³⁰ *Penalty Kick Mgmt. Ltd. v. Coca Cola Co.*, 318 F.3d 1284, 1292 (11th Cir. 2003) (applying Georgia law); *Cognis Corp. v. ChemCentral Corp.*, 430 F. Supp. 2d 806, 812 (N.D. Ill. 2006); *PMC, Inc. v. Kadisha*, 93 Cal. Rptr. 2d 663, 673 (Cal. Ct. App. 2000)

³¹ 下記「差止命令」「損害賠償」を参照

³² *Restatement of Torts*, Section 757, Comment (f)

た場合

- 保有者から、それを許可するライセンスを受けている場合³³
- 公に使用、又は、公衆に供覧されている営業秘密を観察して取得した場合

(2) DTSA

①適正な行為の除外

DTSA は、判例法と同様に、営業秘密の取得、使用又は開示行為が「不正」ではない場合として、以下を規定している³⁴。特に、

- 保有者と独立して営業秘密を取得した場合
- 既に適正に知られていた情報・物件を、リバースエンジニアリングして取得した場合
- その他の適正な取得

②公益目的の除外

さらに、DTSA は、下記の行為は同法により禁止されず、また、同法による民事救済の付与から除外されると規定する³⁵。

- 1) 連邦政府、州政府又はその下部機関により、合法的になされた場合
- 2) 連邦政府、州政府、地方公共団体、又は弁護士に対して、違法行為を通告する、あるいは、捜査する目的だけのために開示され、開示が封印の下にされている場合
- 3) 雇用主による報復行為を裁判で訴えている従業員が、弁護士に対して開示、あるいは、裁判所手続で使用了した場合

なお、上記 2) 及び 3) は、州法に基づく営業秘密侵害の訴えにおいても、侵害にはあたらない理由として主張できるとする。

③雇用主の通知義務

雇用主は、従業員に秘密保持義務あるいは守秘義務を負わせるような契約を締結させたり、合意させたりする場合には、上記の 3) の免責規定を従業員に通知しなければならない。この通知を怠ると、懲罰的賠償や弁護士費用を請求することや補償を受け

³³ 注意として、ライセンスには、明示のライセンスの他に、黙示のライセンスが存在することであり、これらについては、州法の規律するところによる。

³⁴ 18 U.S.C. § 1839(6)

³⁵ 18 U.S.C. § 1833(b)

ることができない。

6 恒久的差止命令等の救済措置における利益調整

UTSA の第 2 条は、営業秘密の侵害が現に行われているか又は差し迫っていると考えられる場合に、差止命令が発せられると規定する³⁶。相手方は、営業秘密が存在しなくなったという事情があれば、命令の取り消しを求めることができる³⁷。

また、同条(b)は、例外的な場合、差止命令に代えて、合理的なロイヤルティの支払いを命じることができるとする。例えば、取得の際には、営業秘密であることや、営業秘密の不正な取得について善意で、認識を欠いていたのに、後に事情を知るに至った場合、その者の使用をすべて禁止するのは、不測の損失を招いてしまい、公平と言い難い。そこで、営業秘密取得時に善意の者に対して、差止命令を発令しないという判断をしようとしている³⁸。

DTSA は、営業秘密の侵害が現に行われているか、又は、差し迫っていると考えられる場合に、妥当と考えられる内容の、侵害を禁止する差止命令が発せられる、と規定する³⁹。相手方が労働者である場合には、雇用の機会を奪う結果となる差止命令は発令できず、営業秘密を侵害する蓋然性、予想される侵害行為等を勘案して、必要かつ合理的な内容の命令でなければならない。他方で、営業秘密保護のための積極的な措置も命ずることができる。

また、衡平の観点から、例外的な場合に、差止命令に代えて、保護が妥当な期間について、合理的なロイヤルティの支払いを命じることができるとする⁴⁰。

7 損害賠償における利益調整

UTSA では、営業秘密取得前の侵害者の立場の変化などを考慮して、衡平に反するという事情の無い限り、営業秘密保有者は、侵害者に対して損害賠償を請求できるとする。

その範囲は、侵害により実際に受けた損失の額、及び、同額に反映されていない侵害者が不当に享受した利益である⁴¹。損害の額は、合理的なロイヤルティの額により算定することもできる⁴²。なお、意図的な、又は、悪意の侵害者に対しては、こうして決せられた損害額の 2 倍を超えない額を懲罰的損害賠償として課しうる⁴³。

³⁶ UTSA 第 2 条

³⁷ UTSA 第 2 条（しかし、侵害者が侵害により利益を受ける **Lead time** の間は、継続させる）

³⁸ UTSA 第 2 条 cmt.

³⁹ 18 U.S.C. § 1836(b)(3)(A)

⁴⁰ 18 U.S.C. § 1836(b)(3)(A)

⁴¹ UTSA 第 3 条

⁴² UTSA 第 3 条(a)

⁴³ UTSA 第 3 条(b)

DTSA でも、営業秘密保有者は、侵害者に対して損害賠償を請求でき、その範囲は、侵害により実際に受けた損失の額、及び、同額に反映されていない、侵害者が不当に享受した利益である⁴⁴。損害の額は、合理的なロイヤルティの額により算定することもできる⁴⁵。また、意図的な、又は、悪意の営業秘密侵害者に対しては、こうして決せられた損害額の 2 倍を超えない額を懲罰的損害賠償として課しうる⁴⁶。

加えて、営業秘密侵害の訴えを誤用・悪用した者、差止命令に対して不当に取消申立てをした者、及び、意図的又は悪意で営業秘密を侵害した者には、弁護士費用を負担させうる⁴⁷。

8 時効

UTSA も DTSA も、営業秘密保有者の請求の時効は、3 年間である⁴⁸。

第 3 章 営業秘密侵害に関連する法律、規制の概要(判例法/UTSA/DTSA 以外)

1 1930 年関税法⁴⁹

(1) 規定対象

関税法には、米国知的財産権の保護や公正な競争確保を目的とする規定として、米国へ輸入される物品については、物品の米国内への輸入、又は、その販売に、不公正な競争方法及び不公正な行為が存在しており、それが米国市場に影響を与える、又は、与える恐れがある場合に、国際貿易委員会（ITC）が調査、決定のプロセスを得て、適当な措置を取ることができるものと定められている。

従って、営業秘密侵害品が輸入されている旨、又は、輸入が予定されている旨の訴えがあり、そのような事実が認められれば、ITC による行政措置の発動が行われ、ひいては、税関により、侵害品の押収が行われることになる。

(2) 捜査と裁判

ITC は、行政府の一部でありつつも、独立した準司法的機関でもあり、行政法判事（ALJ）による審判手続が行われている⁵⁰。調査の申請あるいは職権により調査開始決定がなされ、通知が公告された後、12 か月から 15 か月以内に手続を完結するのが基本である

⁴⁴ 18 U.S.C. § 1836(b)(3)

⁴⁵ 18 U.S.C. § 1836(b)(3)(B)

⁴⁶ 18 U.S.C. § 1836(b)(3)(C)

⁴⁷ 18 U.S.C. § 1836(b)(3)(D)

⁴⁸ UTSA 第 6 条、18 U.S.C. § 1836(d)

⁴⁹ Tariff Act §337(a)(1)(A), 19 U.S.C.A. §1337(a)(1)

⁵⁰ 第 337 条、米国国際貿易委員会 (最終アクセス日 2022 年 2 月 18 日)

https://www.usitc.gov/intellectual_property/about_section_337.htm.

⁵¹。主張（争点）の整理、証拠開示手続は、裁判所で実施されているものと比べると、ずっと迅速に行われる。調査対象となる当事者にとっては、証拠開示がより広範囲にわたりうるため、対応だけでも大変な費用と労力を要するものであり、営業にも支障が生じる。

ITC は、関税法違反行為として調査を行い、違反行為を認める場合には、物品の輸入に対して次のような措置を取ることができる⁵²。

- 物品の輸入の排除
- 暫定的な物品の輸入の排除
- 違反行為の停止
- 手続と証拠開示の濫用に対する制裁
- 物品の押収と没収

2 連邦経済スパイ法⁵³

1996 年に制定された連邦経済スパイ法は、海外の政府や機関を利する、営業秘密の取得、開示、使用する行為を連邦犯罪とし、違反行為に対する懲役、罰金の法定刑を規定する。連邦政府の刑事訴追の根拠となり、また、司法省が、違反行為の差止命令を、民事事件として求めることもできることも規定されている。

(1) スパイ目的の営業秘密侵害⁵⁴

- a. 犯罪が外国政府、外国の機関又は外国の代理人に利益をもたらすことを意図して、あるいは、それを知る者が、故意に
 - i. 盗む、若しくは、許可なく、流用する、取得する、持ち去る、あるいは、隠す、又は、偽り、欺き、又は、欺瞞によって、営業秘密を取得する
 - ii. 許可なく、営業秘密のコピー、複製、スケッチ、描画、撮影、ダウンロード、アップロード、変更、破棄、複写、模造、送信、配信、送付、郵送、通信、又は伝達する
 - iii. 営業秘密を、それが、盗まれ、若しくは、許可なく流用、取得、あるいは、変換されたことを知って、受取り、購入、所持する。
 - iv. 上記第（a）項から（c）項のいずれかに記載されている違反を犯そうとす

⁵¹ 第 337 条調査の質問と回答、米国国際貿易委員会 (最終アクセス日 2022 年 2 月 18 日) https://www.usitc.gov/intellectual_property/documents/337_faqs.pdf.

⁵² 米国内において、下記危害やその恐れが起こることが必要である。(i) 米国の産業を破壊、又は、実質的に損なうこと、(ii) そのような産業の確立を防げる、(iii) 米国の貿易、および、商取引を制限、又は、独占する

⁵³ 18 U.S.C. §§ 1831,1832

⁵⁴ 18 U.S.C. § 1831

る

v. 上記第 (a) 項から (c) 項のいずれかに記載されている罪を犯すために、1 人以上の他者と共謀し、その 1 人以上が、共謀の目的を達成するために、行為を行う場合には、次項 (b) の場合を除き、500 万ドル以下の罰金、15 年以下の懲役、又は、その両方を科す。

b. 第 1 項(上記の a) に違反した組織には、1,000 万ドル、又は、営業秘密の研究、デザイン、その他必要となる費用の回避分を含む、盗まれた営業秘密の価値の 3 倍を超えない額のいずれか高い金額で罰金を科す。

(2) 非スパイ目的（産業スパイ）の営業秘密侵害⁵⁵

a. 営業秘密を領得する目的で、州間取引若しくは外国取引で使用される、又は、使用予定である、製品、若しくは、サービスに関連して、その所有者以外の者の経済的利益に、営業秘密の所有者に不利益を与えることを、意図し、あるいは、知りながら、故意に、前条の行為を犯す場合に、罰金、10 年以下の懲役、又は、その両方を科す。

b. 第 1 項(上記の a)に違反した組織には、500 万ドル、又は、営業秘密の研究、デザイン、その他必要となる費用の回避分を含む、盗まれた営業秘密の価値の 3 倍を超えない額のいずれか高い金額で罰金を科す。

(3) 没収規定

連邦経済スパイ法は、侵害品の没収、破壊、被害者への返還ができることを規定する⁵⁶。

(4) 時効

連邦経済スパイ法違反の時効は、5 年間とされている⁵⁷。

(5) 州刑事法との関係

連邦経済スパイ法は、州間の取引、国際取引に関わる製品やサービスに適用される⁵⁸。この条件自体は充たされることは少なくないと考えられる（営業秘密の侵害に係る製品やサービスが一つの州だけにとどまっているのは少ない）が、連邦経済スパイ法の処罰の対象は上述のとおり、故意による所定の営業秘密の取得、開示、及び、使用に限られている。

⁵⁵ 18 U.S.C. § 1832

⁵⁶ 18 U.S.C. § 1834

⁵⁷ 18 U.S.C. § 3282

⁵⁸ 18 U.S.C. §§ 1831, 1832

3 州刑事法

営業秘密侵害を刑事犯罪として処罰する州は少なくはない⁵⁹。そして、懲役刑や罰金刑が法定刑として規定され、実際に刑事処罰が行われた歴史を有している。以下詳しく述べる。

(1) 営業秘密の定義

州法の営業秘密の定義は統一されていないが、カリフォルニア州を含め、かなりの州は、ニュージャージー州の定義と類似した定義を採用している⁶⁰。他方、近年になって営業秘密侵害を犯罪化した州では、UTSA に沿った定義を採用している⁶¹。ニュージャージー州の定義は、科学的情報、又は、技術的な情報を保護対象とするが、顧客情報や財務情報は含まないと考えられており、UTSA より狭くなっている。

(2) 侵害行為

侵害行為としては、殆どの州で、窃盗罪の構成要件とほぼ同じ行為を犯罪とする。特に、主観的要件として、営業秘密保有者から、その財物を奪取する意図を要求するものが殆どである。

(3) 重罪化

幾つかの州で、軽犯罪ではなく、重罪（通常の刑事犯罪）となるために、取得された営業秘密の価値が、一定額以上であることを必要とする。例えば、アラスカ州、アイオワ州、ノースダコタ州、オレゴン州、サウスダコタ州では、通常の刑事事件として立件されるためには、営業秘密の価値が 1,000 ドル以上であることが証明されなければならない⁶²。

(4) 法定刑

州により、最高の懲役や罰金の多寡は違っている。厳罰化が見られるミズーリ州では、最高 15 年の懲役、5,000 ドル、又は、侵害者の利益の 2 倍までの罰金を課せうとされ、デラウェア州では、最高 25 年の懲役、妥当な場合には罰金、それに被害者への犯罪収益の返還を命じうる⁶³。

⁵⁹ 50 年を超える歴史を有する州もある。Kurt M. Saunders & Michelle Evans, A Review of State Criminal Trade Secret Theft Statutes, 21 UCLA J.L. & Tech. 1, 2-3 (2017)

⁶⁰ 多くは、次のように定義する。秘密であることで価値のある、科学的又は技術的な情報、設計、プロセス、手順、公式又は改善。そして、限られた目的のためにアクセスできる、指定された人以外の人ができるようになることを防止する措置を、所有者が講じる場合、営業秘密は、秘密であると推定される。Saunders & Evans, 7-8

⁶¹ Saunders & Evans, 7-8

⁶² Saunders & Evans, 7-8

⁶³ Saunders & Evans, 7-8

4 秘密保持条項違反

(1) 一般原則

労働契約などで、侵害者が秘密保持義務を負うとの合意が存在し、契約上の義務違反として、営業秘密又は機密情報保持義務違反を訴える場合、各州の判例法によらなければならない。

各州の裁判例は、企業間での秘密保持条項と労働者との秘密保持条項とで、異なったアプローチを取る。前者では、契約条項をなるべく忠実に解釈するのに対して、後者では、従業員であった者の自由な市場参加への拘束が、非合理的な市場取引の制限にあたらないか精査される⁶⁴。具体的には、退職した労働者が機密情報や営業秘密を使用することを制限する条項に、「合理性」があることを必要とする⁶⁵。

事案により異なるものの、条項があまりに広すぎる場合には、(1)秘密保持義務が課されるのは、営業秘密に該当するような、機密性の高い情報にのみであるとして、問題の情報は、秘密保持義務の範囲外であったとしたり、(2)差止命令を狭い範囲でのみ発令する、という措置をとる⁶⁶。あるいは、(3)秘密保持条項は、不公正な取引にあたるとして、法的拘束力を否定することもある⁶⁷。したがって、広い情報を「機密情報」としてカバーしうる定義を設けることは、保有者にとって重要であるが⁶⁸、あまりに無制限に含めるのは逆効果である。

(2) 必然的開示の原則

ペンシルバニア州、イリノイ州、アイオワ州、ニューハンプシャー州など、幾つかの州で、前雇用主の重要な機密情報に接することのできた従業員が、競合相手の営業上重要な地位に転職してしまうことを、「営業秘密を必然的に開示してしまう」と推定し、禁止することを認めている⁶⁹。個別の事案によるが、元従業員の労働の自由を制限する可能性はあり、州が判例を変更する内容の労働者保護法を定めることがある⁷⁰。

(3) 差止命令による救済

元従業員等、秘密保持義務を負う者が、営業秘密を開示あるいは使用してしまう可能性が

⁶⁴ North Pacific Lbr. Co. v. Moore, 275 Or. 359 (1976)、Ticor Title Ins. Co. v. Cohen, 173 F.3d 63 (2d Cir. 1999)

⁶⁵ BDO Seidman v. Hirshberg, 93 N.Y.2d 382 (1999); Eldridge v. Johnston, 195 Or. 379 (1952)

⁶⁶ 雇用後も、営業秘密に対する秘密保持義務を負うが、仕事から得られたスキルや知識は、含まれない。広すぎる条項は、過剰な義務を課す部分を、無効化して解釈されることがある。

BDO Seidman v. Hirshberg, 93 N.Y.2d 382 (1999)

⁶⁷ Geloff v. R.C. Hemm's Glass Shops, Inc., 167 N.E.3d 1095 (Ohio Ct. App. 2021)

⁶⁸ Synthes, Inc. v. Emerhe Med. Inc., 25 F. Supp. 3d 617 (E.D. Pa. 2014)

⁶⁹ PepsiCo, Inc. v. Redmond, 54 F.3d 1262 (7th Cir. 1995)

⁷⁰ マサチューセッツ、イリノイ州など。

ある場合には、差止命令が発令されうるが、裁判所は、営業秘密侵害事件に比較して、その妥当性や範囲につき、慎重に判断する傾向がある⁷¹。

(4) 競業避止義務違反

秘密保持義務と同様、あまりに広い内容の競業避止義務は「合理性」を欠くため、全部又は一部が無効となる。その他にも、判例により形成されてきた法理あるいは原則が存在し（競業避止義務を課すべき必要性や合理性がないとする事情がある）、一定の場合に、条項が無効とされることがある⁷²。

5 通信関連機器に関する刑事法

(1) コンピューター犯罪取締法（1986）

類型と法定刑		
犯罪となる行為	法定刑	コメント
国家機密を取得する (a) (1)	10 年	
不正アクセスし情報を取得する (a) (2)	原則 1 年、一定の加重事由あれば 5 年	1030(a)(2)(C)は、意図的に、権限なく、あるいは権限を超えて、保護されたコンピューターにアクセスし、保護されたコンピューターから、情報を取得した場合、州間又は外国の通信が含まれる場合は、違反する。
政府コンピューターへの侵入 (a) (3)	1 年	
詐欺又は利益取得目的でのアクセス (a) (4)	5 年	コンピューターの使用自体は詐欺あるいは利益取得に含まれず、利益取得が 1 年に 5,000 ドルを超えない場合には、該当しない。なお、詐欺の目的は、不法領得のみならず、不誠実を示す主観的要素で足りるとする裁判例がある。 ⁷³
情報送信を故意に行うことで、保護されたコンピューターへ意図的に危害を与える (a) (5) (A)	1 年か 10 年	送信するのは、プログラム、情報、コードなど。営業秘密の送信が、コンピューターのデータの整合性の破壊とい

⁷¹ Cabela's LLC v. Highby, 362 F. Supp. 3d 208 (D. Del. 2019), aff'd, 801 F. App'x 48 (3d Cir. 2020)

⁷² Rector-Phillips-Morse, Inc. v. Vroman, 253 Ark. 750 (1973)

⁷³ Shurgard Storage Centers, Inc v. Safeguard Self Storage, Inc 119 F. Supp. 2d 1121 (WD Wash. 2000)

		う損害にあたるとする裁判例もある。 ⁷⁴
故意に保護されたコンピューターにアクセスし、無謀に((a) (5) (B))又は、過失で危害を与える(同(C))	原則 1 年、一定の加重事由あれば 5 年	
パスワードの取引(a) (6)	1 年	
コンピューターに関する脅迫(a) (7)	5 年	
上記の未遂や共謀(b)	10 年	

米国連邦法として、コンピューター犯罪取締法が制定されており、第三者の管理するコンピューターにアクセス権限が無い、又は、アクセス権限を超えてアクセスすることを禁止する⁷⁵。犯罪として捜査、告訴されることがあるが、民事訴訟を提起し、(1) 法の規定する犯罪類型に該当する行為の存在、(2) 損害又は損失を被ったことを主張、立証して、損害賠償請求をすることも可能である⁷⁶。なお、「保護された」コンピューターという概念が重要であり、情報自体が営業秘密として保護されていたかどうかは、犯罪の成否に影響しない。

(2) 電信詐欺法・郵便詐欺法⁷⁷

電信機器、ラジオ、テレビ等を用いた組織的な詐欺、及び、郵便を用いた組織的な詐欺は、連邦犯罪として、それぞれ懲役 20 年、懲役 30 年の法定刑が規定されている。

6 営業秘密事件の審理と措置

(1) 一時的抑制命令⁷⁸

⁷⁴ Shurgard Storage Centers, Inc v. Safeguard Self Storage, Inc 119 F. Supp. 2d 1121 (WD Wash. 2000)

⁷⁵ 18 U.S.C. § 1030

⁷⁶ 18 U.S.C. § 1030(g) 18 U.S.C. § 1030(a)(5)(B)(i),(ii),(iii),(iv),又は(v)に記載されている要因の 1 つが、行為に含まれる場合にのみ可能であり、(i) は経済的損害に限定される。

⁷⁷ 18 U.S.C. §§ 1341,1343

⁷⁸ 連邦民事訴訟規則第 65 条(b)

カリフォルニア州では、証拠により、以下の要件が充たされれば、営業秘密の侵害に対する一時的抑制命令あるいは暫定的差止命令を発令する。Whyte v. Schlage Lock Co., 101 Cal. App. 4th 1443, 1463–64 (2002); Prime Tech Staffing v. Mickelsen, 2005 WL 775688, *3+ (2005) ニューヨーク州でも、同等の要件である。N.Y. C.P.L.R. 6301

- 申立人が、本家で勝訴する可能性（これに関して、営業秘密の特定や、合理的な秘密性保持の措置が問われる）
- 命令が認められない場合、申立人に生じる取り返しのつかない損害(侵害が行われる切迫性)
- 上記の 2 要素のバランスー命令が認められた場合に侵害者に与えると予測される損害に比較して、命令が認められない場合に生じると予測される申立人の損害の超越

営業秘密保有者は、裁判所に対し、一時的抑制命令を申し立てることができ、侵害行為の停止や侵害品等の証拠の保全を命じるように、請求することができる⁷⁹。

一時的抑制命令は、侵害者の関与なく、申立人のみが関与する一方的な手続を経て、発せられることもできる。その場合、申立人は以下を主張・立証する必要がある⁸⁰。

- a. 営業秘密侵害の本案で勝訴する相当な蓋然性、
- b. 命令が認められない場合、申立人に生じる取り返しのつかない損害
- c. 命令が認められた場合に侵害者に与える損害に比較し、命令が認められない場合に生じる申立人の損害が上回ること、
- d. 公共の利益

一時的抑制命令は、被申立人に生じうる損害を補償するための保証金を、申立人が提供しなければ発せられない⁸¹。

また、一時的抑制命令は、最大で 14 日間のみ存続する。被申立人に通知することなく発せられた場合は、被申立人が参加する暫定的差止命令審尋期日を予定しなければならない。

(2) 暫定的差止命令⁸²

営業秘密保有者は、裁判所に対し、暫定的差止命令を申し立てることができ、侵害行為の停止や証拠の保全、侵害品等の差押え、物品の中立した第三者による保管を命じるように、請求することができる⁸³。

暫定的差止命令は、申立人が被申立人に通知し、被申立人が関与する審尋手続を経て発せられることが原則である。その場合、申立人は、以下を主張・立証する必要がある⁸⁴。

- a. 営業秘密侵害の本案で勝訴する相当な可能性、
- b. 命令が認められた場合に侵害者に与える損害に比して、命令が認められない場合に生じる申立人の損害が上回ること
- c. 命令が認められない場合、申立人に生じる取り返しのつかない損害
- d. 公共の利益

⁷⁹ *Schiavo ex rel. Schindler v. Schiavo*, 403 F.3d 1223, 1225–26 (11th Cir. 2005).

⁸⁰ *Schiavo ex rel. Schindler v. Schiavo*, 403 F.3d 1223, 1225–26 (11th Cir. 2005).

⁸¹ 連邦民事訴訟規則第 65 条(c)

⁸² 連邦民事訴訟規則第 65 条(a)

⁸³ 連邦民事訴訟規則第 65 条(a)

⁸⁴ *Beacon Theatres, Inc. v. Westover*, 359 U.S. 500, 506–07 (1959)、*Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7 (2008)

ニューヨーク州では、明白で説得力のある証拠により、以下が立証されると、暫定的差止命令を発令する。N.Y. C.P.L.R. 6301; *Arthur J. Gallagher & Co. v. Marchese*, 946 N.Y.S.2d 243, 244 (2d Dep’t 2012).

- 申立人が、本案で勝訴する可能性（これに関して、営業秘密の特定や、合理的な秘密性保持の措置が問われる）
- 命令が認められない場合、申立人に生じる取り返しのつかない損害(侵害が行われる切迫性)
- 衡平の観点から、申立人の利益が被申立人の利益を超越

暫定的差止命令は、被申立人に生じうる損害を補償するための保証金を、申立人が提供しなければ、発せられない⁸⁵。

(3) 本案前証人尋問請求⁸⁶

訴訟を提起する前にも、証拠が逸失してしまいかねない場合には、証人から証言を得る手続を裁判所に申立て、証言を保全することができる。これは、相手方に通知することを要し、下記を示さなければならない。

- 申立人が訴訟提起を予定しているが、現在それを提起することはできないこと
- 予定される訴訟の本質及びそれに対する申立人の利害
- 証言が示すと予想される事実とその取得を望む理由
- 予想される不利な当事者の名前と住所
- 証言録取される者の名前と住所及び予想される証言内容

(4) 連邦裁判所に対する証拠品、侵害品の差押えの申立て⁸⁷

DTSAにおいて、営業秘密保有者は、連邦裁判所に対して、相手方に対する通知を得ない申立てを行い、相手方の財産を差し押さえる命令を得ることができる。この一方的な差押申立手続は、本案訴訟の証拠を保存するため、又は、営業秘密の伝播又は拡散がされないようにするために利用される。申立人が、以下の事実を証拠で証明した場合に、裁判所は、相手方からの証拠を差押え、移動して保管することができる。

- a. 相手方が回避するか、従わない可能性が高いため、一時的抑制命令では不十分である
- b. 申立てが認められない場合、即時で回復不可能な損害が、申立人に発生する
- c. 申立てを否定することによる申立人への損害は、申立てが認められて、命令を受ける者の正当な利益を上回り、および、命令によって影響を受ける可能性のある第三者への損害を有意に上回る
- d. 営業秘密が存在する
- e. 相手方が、営業秘密を侵害しているか、若しくは、侵害の恐れがあり、あるいは、これらを企図している
- f. 営業秘密と差押対象とされる物を、相手方が所持している
- g. 差し押えられる対象とその場所を合理的に特定している
- h. 相手方、及び、相手方に加担している者は、申立手続の通知を受けると、対象物を破壊、移動、隠匿するか、さもなければそれに裁判所がアクセスできないようにする
- i. 申立人は、要求する差押を公表していない

以上の要件は、一時的抑止命令（同様に、一方的な手続で発令されうる）に比して、非常に厳格であり、これらを十分に証明することは、多くの場合に難しいと思われる⁸⁸。

⁸⁵ 連邦民事訴訟規則第 65 条(c)

⁸⁶ 連邦民事訴訟規則第 27 条

⁸⁷ 18 U.S.C. § 1836(b)(2)

⁸⁸ Klapow, et al. 脚注 4

(5) 訴訟手続における証拠開示、営業秘密の保護

米国では、民事事件の本案が提起され、最初の被告の答弁あるいは訴訟却下の申立てがされた後、証拠開示に関する当事者間のやりとりが始まる⁸⁹。したがって、営業秘密保有者としては、訴状の作成、裁判所への提出の段階では通常、相手方たる私人から、公的な経路で情報を入手することはできない⁹⁰。

証拠開示にあたり、営業秘密保有者は、裁判所の保護命令を求めることができる⁹¹。保護命令申立てには、営業秘密の保護以外も、保護を求める理由とすることができ、当事者又は個人を、支障、困惑、抑圧、又は、過度の負担、若しくは、費用から保護するため、保護命令が必要とする正当な理由があることを主張し、証明する⁹²。裁判所は、以下を命じうる。

- a. 開示又は見分を禁止する。
- b. 開示又は見分のために、時間と場所又は費用の配分を含む条件を指定する。
- c. 開示を求める当事者によって選択された方法以外の方法を指示する。
- d. 特定の事項についての調査を禁止又は開示、若しくは、見分の範囲を特定の事項に限定する。
- e. 見分が行われている間に、立ち会う可能性のある人物を指定する。
- f. 裁判所の命令があった場合にのみ、証言録取書を封印して、開封することを要求する。
- g. 営業秘密又はその他の機密の研究、開発、又は商業情報が開示されないこと、又は特定の方法でのみ開示されることを要求する。
- h. 裁判所の指示に従って開封するために、当事者が指定された文書又は情報を、封印された封筒で同時に提出することを要求する。

保護命令が発せられると、保有者は、自己の主張・立証にあたり、保護命令が指定する、営業秘密や機密情報の開示の方法、アクセス制限に従って、関連する書面やデータに、営業秘密、又は機密情報が含まれていないか確認し、もし含まれていれば、その旨を特定、説明等することとなる。

争いが生じれば、裁判所は、イン・カメラ手続（公衆の傍聴できる公開廷でなく、当事者と裁判官のみで、秘密性を判断する手続）を用いて、実際の証拠等に機密情報等が存在するかを判断することもできる⁹³。

⁸⁹ 連邦裁判所の事件の場合、連邦民事訴訟規則第 26 条

⁹⁰ 相手方に原告の代理人が非公式に接触することもあるが、営業秘密侵害事件での、このような交渉の行われる割合は、不明である。

⁹¹ 連邦民事訴訟規則第 26 条 実務では、各裁判所及び裁判官が、定形の規則として、保護命令に等しい内容を含む命令を予め作成して、当事者に適用しているのが通常である。

⁹² 連邦民事訴訟規則第 26 条

⁹³ UTSA 第 5 条

DTSA はこうした判例法の用意する秘密保護のシステムに加え、裁判所が、積極的に営業秘密保有者が営業秘密と主張する情報を、十分に保護する措置を採用しなければならないと規定する⁹⁴。

(6) 恒久的差止命令

① 判例法⁹⁵

UTSA が規定するように、営業秘密が侵害されている、又は、侵害の恐れがあると認められる場合、裁判所は、恒久的差止命令を命じることができる⁹⁶。そして、例外的な状況があれば、差止めの認められ得る期間を超えない期間について、被告による合理的なロイヤルティの支払いを命じることできる⁹⁷。

判例法上、原告が本案（主な手続き）の請求を基礎づける事実の立証に成功すれば、*eBay* 判決の示した要件に基づき、営業秘密保有者たる原告への救済手段として、以下を命じることができる⁹⁸。

- a. 営業秘密の開示、利用の禁止、
- b. 営業秘密を含む、若しくは、具体化する、侵害者が所持、若しくは、所有する文書、物件、材料、物質、又は電子ファイルの破壊、又は所有者への返還
- c. 侵害品のリコール、破壊、流通経路からの侵害製品の除去
- d. 侵害者の関連業務における営業秘密の混入、使用の防止のために必要なあらゆる措置、必要な場合、特定の従業員の隔離、誓約、監視、検証の措置

② DTSA⁹⁹

DTSA では、以下に記載する要件と制限の下に、民事救済として、恒久的差止命令を命じることができると規定する。

- a. 実際の、又は、恐れのある営業秘密侵害を防止するために、裁判所が合理的であるとみなす条件を、下記に従って課す
 - i. 被告が、雇用関係に入るのを防ぐことなく、また、雇用に課せられる条件が、被告が知っているとする情報だけでなく、侵害事実を示す証拠に基づいている
 - ii. 上記以外の場合は、合法的な職業、取引又はビジネスに対する制約を禁止する、適用州法に反しない

⁹⁴ 18 U.S.C. § 1835

⁹⁵ 上記 3.6 「恒久的差止命令等、救済措置における利益調整」を参照

⁹⁶ UTSA 第 2 条

⁹⁷ UTSA 第 2 条(b)

⁹⁸ *Marine Turbo Engineering, Ltd. v. Turbocharger Services Worldwide, LLC*, No. 11-60621-CIV, 2012 WL 13005811 (S.D. Fla. July 23, 2012)

⁹⁹ 18 U.S.C. § 1836(b)(3)(A)

- b. 裁判所によって適切と判断された場合、営業秘密を保護するために、積極的な措置を講じることを要求する

ただし、例外的な状況があれば、救済措置の認められ得る期間を超えない期間について、合理的なロイヤルティの支払いを命じることもできることについては、上述したとおりである。

7 損害賠償

(1) 判例法

UTSA では、営業秘密保有者は、侵害者に対して、侵害により実際に受けた損失の額、及び、同額に反映されていない、侵害者が不当に享受した利益を、侵害者に対して請求することができる¹⁰⁰。損害は、合理的なロイヤルティの額により、算定することもできる¹⁰¹。

(2) DTSA

DTSA では、営業秘密保有者は、侵害者に対して、侵害により実際に受けた損失の額、及び、同額に反映されていない、侵害者が不当に享受した利益を、侵害者に対して請求することができる¹⁰²。損害は、合理的なロイヤルティの額により算定することもできる¹⁰³。

第4章 営業秘密事件の実務

1 保護される営業秘密

営業秘密の定義に関して、多くの裁判例を鑑みると、DTSA の定義が、UTSA の定義と同様であることを重視して、UTSA を採用して制定された、各州営業秘密法に基づく各州の判例は不変であり、過去の判例を引き継ぐものと理解されている¹⁰⁴。

営業秘密を具現化した製品が写真で公表されたり、一部の情報は特許として保護されていたりしても、それ自体で営業秘密を消失させるわけではないため、被告としては注意が必要である¹⁰⁵。

¹⁰⁰ UTSA 第3条

¹⁰¹ UTSA 第3条(a)

¹⁰² 18 U.S.C. § 1836(b)(2)(C)

¹⁰³ 18 U.S.C. § 1836(b)(2)(C)

¹⁰⁴ *Midwest Sign & Screen Printing Supply Co. v. Dalpe*, 386 F. Supp. 3d 1037, 1053 (D. Minn. 2019); *Kuryakyn Holdings, LLC v. Ciro, LLC*, 242 F. Supp. 3d 789, 797-98 (W.D. Wisc. 2017); *Earthbound Corp. v. MiTek USA, Inc.*, 2016 WL 4418013, at *10 (W.D. Wash. Aug. 19, 2016)

¹⁰⁵ *T-Mobile USA, Inc. v. Huawei Device USA, Inc.*, 115 F. Supp. 3d 1184, 1193 (W.D. Wash. 2015)

実務上最も問題となるのは、原告が、証拠開示を経ていない訴訟提起段階で、どの程度詳細に被告が侵害したとする営業秘密を特定しなければならないかである。被告が、具体的にどのようにして取得したか、どのように使用しているかについては殆ど分からないが、ある程度、被告がアクセスできた情報について原告で推測がついている場合には、営業秘密を広く定義しても、訴訟が却下されないことが多い¹⁰⁶。しかし、広範すぎることによって、主張立証の対象が定まらない場合には、請求が却下されてしまう¹⁰⁷。

侵害の対象である営業秘密の範囲について、ニューヨーク州は、訴状の記載において、被告に対して、何の侵害で訴えられたかを知らせるに足りる十分な特定性を要求し¹⁰⁸、カリフォルニア州では、合理的な特定性を要求する。このように、表現上の違いはあるが、技術分野によっても、原告と被告の関係によって、裁判所のアプローチは異なっていると考えられ、実務上の差異は明らかではない¹⁰⁹。

2 営業秘密侵害行為の認定

(1) 違法な「使用」の範囲：原告との契約内容、被告の侵害品

違法な「使用」にあたるかは、もし契約関係が存在する場合には、原告と被告（又は被告関連会社）との契約内容、被告の提供する（予定の）侵害品の性状が、重要な判断要素となる。

テキサス州最高裁は、保有者に不利益となりうる営業秘密の商業的利用である限り、「使用」として、侵害行為を構成すると判示した¹¹⁰。これに準じ、第5連邦巡回控訴裁判所も、ライセンス切れとなったコンピューターを解析、使用して、自社の製品を作るという、侵害品の製造行為は、研究・開発上の使用、情報を利用した新規顧客開拓と並んで、違法な「使用」と考えられると判断した¹¹¹。ニューヨーク州の連邦破産裁判所も、契約上の守秘義務、

¹⁰⁶ 原告の顧客リスト、顧客の価格設定、過去の販売実績等は十分に特定されているとした判例、*Brocade Commc'ns Sys., Inc. v. A10 Networks, Inc.*, 873 F. Supp. 2d 1192 (N.D. Cal. 2012), on reconsideration in part, No. C 10-3428 PSG, 2012 WL 12925716 (N.D. Cal. July 8, 2012)

¹⁰⁷ 原告が、6頁にわたり、行間なく、内部機密情報の項目を羅列した場合、*AMP Inc. v. Fleischhacker*, 823 F.2d 1199, 1203 (7th Cir. 1987)に許可したり、数千もの営業秘密のうち、問題となっている情報を大まかに特定した場合、*Litton Sys., Inc. v. Sundstrand Corp.*, 750 F.2d 952, 954, (Fed. Cir. 1984)、原告が54頁に103件の営業秘密を列挙した場合、*Struthers Scientific & Int'l Corp. v. General Foods Corp.*, 51 F.R.D. 149, 151-52 (D. Del. 1970)。

¹⁰⁸ *PaySys Int'l, Inc. v. Atos Se*, No. 14-CV-10105, 2016 WL 7116132 (S.D.N.Y. Dec. 5, 2016)

¹⁰⁹ Cal. Civ. Proc. Code §2019.210

¹¹⁰ *Computer Assocs. Int'l v. Altai, Inc.*, 918 S.W.2d 453, 455 (Tex.1996)

¹¹¹ *Gen. Universal Sys., Inc. v. HAL, Inc.*, 500 F.3d 444, 450-51 (5th Cir. 2007)

秘密保持義務が、不正「使用」に該当するかどうかの判断で、吟味されると判示した¹¹²。

第 11 連邦巡回控訴裁判所も、「使用」「開示」を広義に解釈して、(i) 第三者が営業秘密を知ることを可能にする情報を提供することは、「開示」であり、(ii) 営業秘密の「相当な部分」を使用して、営業秘密から「相当に由来した」改善、若しくは、修正を作成する行為は、「使用」であり、他方、営業秘密から「わずかな」貢献のみで、具体化されたとされる物品を製造した場合、使用の責任を負わないと判示した。このように、侵害品の性状と営業秘密の性状・内容の比較をスライディング・スケールで行い、不正な「使用」かどうかを判断する意見が多い。

カリフォルニア州第 6 地区控訴裁判所は、原告が、自己のソフトウェア製品に関する特定の技術情報、Cookie のバッファリング、セッションの維持、セッションの破棄、負荷分散などのソフトウェアに関する技術的に詳細な事項を、被告の質問に回答する形で開示していた場合、被告が自己の事業に密かに応用、改良していた場合には、「使用」に当たるとした¹¹³。反対に、原告が、機密保持契約下に、健康保険の窓口の事務が一般にどのように機能するのかを説明したり、自己のデータ入力、出力がどうなっているのかを見せたりするだけでは、被告が後に自社製品を開発したとしても、違法な「使用」の内容とはならないと判断した¹¹⁴。

(2) DTSA による営業秘密侵害行為の拡大

DTSA に関しての判決は、以下の点で、新法が侵害行為の範囲を広げると考えることもできる。

① 「不正使用を達成させる行為」

DTSA の営業秘密侵害の定義には、営業秘密の不正使用を「達成させる」行為が含まれる。この点について、裁判所は、用語が意味する行為は、犯罪行為の計画が開始されてから、犯罪完了に至るまでの、犯罪が遂行中であることを明らかにする如何なる行為も含めて解釈されるべきと判断した。そこで、被告が、多くの国内展示会で、不

¹¹² *In re Collins*, 540 B.R. 54, 63 (Bankr. E.D.N.Y. 2015)

¹¹³ 原告は、機密保持契約に従って、ソフトウェア製品を被告に販売する過程で、ソフトウェアに関する、個別化された、非常に具体的な事実を、被告に開示し、追加の内容を含む、技術バインダーを被告に提供した。原告のソフトウェア製品に関する特定の技術情報として「Cookie のバッファリング」、「セッションの維持」、「セッションの破棄」、「負荷分散」、「その他の事項」などのソフトウェアに関する技術的な質問に回答した。 *Ajaxo, Inc. v. E*Trade, Inc.*, 135 Cal.App.4th 21, 37 Cal.Rptr.3d 221, 227–229 (6th Dist. 2006)

¹¹⁴ *Agency Solutions.Com, LLC v. TriZetto Grp., Inc.*, 819 F. Supp. 2d 1001, 1029–30 (E.D. Cal. 2011)

正取得されたとされる、営業秘密を具体化した製品を宣伝、促進、販売してきた以上、「不正使用」がされたと認定した¹¹⁵。しかし、この DTSA の「達成させる」行為には、他者の営業秘密の侵害行為を幫助する行為は含まれていないとする下級審レベルの判決も存在している¹¹⁶。

即ち、現在のところ、DTSA に関する裁判例で、侵害行為を広義に解釈する判決が下されてきているものの、具体的な事案の事実関係により判断が分かれると予想され、今後の裁判例の発展を見極める必要がある。

② 不法な使用、開示、取得の行為地

海外法人である被告が、米国法人である原告の営業秘密を、原告の海外子会社の従業員から取得し、米国内のトレードショーで侵害品を展示した事件で、イリノイ州の連邦裁判所は、DTSA が、被告らの行為に適用される根拠として、DTSA の域外適用に関する 1837 条は、RICO 規定と異なり、行為と米国との結合性を要求しておらず、また、DTSA は、不正取得が DTSA の施行前の場合でも適用されるので、不正使用が施行後である以上、不正使用により生じた損害賠償の請求や不当利得の返還を求めることができると判断した。即ち、域外での使用行為についても、損害賠償を可能とすると解釈した¹¹⁷。

3 訴訟提起及び証拠収集段階における営業秘密の保護

米国の民事訴訟法は、訴訟提起段階では、厳格な請求の原因の特定を要求しないが、ディスカバリー（証拠開示）が不当に広範にならない程度の「営業秘密」の限定が必要であり、侵害されたと主張する「営業秘密」の内容を次々と変更することは、心証形成に悪影響を与えかねない¹¹⁸。ビデオのクラウドに関連する技術を保有していた原告が、ビデオのクラウドのアーキテクチャ及び技術を利益化する手法が営業秘密であったとして、被告を訴えた事件で、個別の要素（コンポーネント）がどう機能するかは示したものの、それが一体としてどのように作動するか等を示せなかった場合に、営業秘密の特定はなかったと判断した裁判例がある¹¹⁹。

¹¹⁵ Motorola Sols., Inc. v. Hytera Commc'ns Corp., 436 F. Supp. 3d 1150, 1164–65 (N.D. Ill. 2020)

¹¹⁶ Power Home Solar, LLC v. Sigora Solar, LLC, No. 3:20-CV-00042, 2021 WL 3856459, at *10 (W.D. Va. Aug. 30, 2021)

¹¹⁷ Motorola Sols., Inc. v. Hytera Commc'ns Corp., 436 F. Supp. 3d 1150, 1162 (N.D. Ill. 2020)

¹¹⁸ Next Commc'ns, Inc. v. Viber Media, Inc., 758 F. App'x 46, 49 (2d Cir. 2018)

¹¹⁹ Next Commc'ns, Inc. v. Viber Media, Inc., 758 F. App'x 46, 49 (2d Cir. 2018)

この裁判例では、被告との間に、機密情報を非常に広く定義する秘密保持契約が存在したが、同契約は、特に営業秘密の存在の立証に有益な要素とはならなかった。

訴状を、機密情報を含めたものを「封印下に」提出することもでき、営業秘密保護のために、多くの事件で利用されているようである¹²⁰。

連邦第6巡回控訴裁判所は、DTSAの規定に基づき、機密性の保護に利用される封印について、封印されて提出された資料が、控訴審で利用される場合でも、封印されたままの状態が維持される旨を判示した。この事件では、従前に特許侵害訴訟を提起し、被告会社と和解した営業秘密保有者が、被告会社と弁護士が和解契約の秘密保持義務に違反して、営業秘密を被告会社の従業員に開示したと主張し、一時的抑制命令を得たが、その後の審理で命令が取り消されたため、控訴したというものである¹²¹ (McKeague, J.)。

元従業員が競争会社に転職した後、元従業員と競争会社による営業秘密侵害の疑いを持ち、訴訟提起のための情報を得るために、連邦民事訴訟規則 27 条（訴訟前の証拠開示）に基づいて、元従業員らから、競争会社の機密情報となっている PortfolioDefense というソフトの開示を求めようとしたところ、裁判所は、当該情報は、テキサス州証拠法 507 条で保護される営業秘密にあたるとして、申立てを却下した¹²²。即ち、州法レベルでの秘密情報の保護規定で、営業秘密侵害訴訟に関する証拠収集を排除した。

4 救済手段、営業秘密保護の現状

前述のとおり、営業秘密侵害行為の被害者である保有者に認められる救済手段としては、従来より、金銭的賠償、不当利得返還、恒久的差止命令、暫定的差止命令、一時的抑止命令が認められてきた¹²³。

(1) 差止命令

営業秘密保持者は、侵害品の破壊、侵害品の引渡し、侵害者からの営業秘密の返還や消去を、差止めで求めなければならない事情を証明できれば、侵害行為を実効的に阻止することができる。

他方で、救済を与えるにあたり、他の法益とのバランスが重要であり、UTSA でも、DTSA でも、侵害者が、当初は、営業秘密の侵害の事実について善意であった場合などは、差止命令に代えて、合理的なロイヤルティの支払いを命じうるとしている。

¹²⁰ 即ち、秘密部分は、黒塗りされ、一般が閲覧できない。T-Mobile USA, Inc. v. Huawei Device USA, Inc., 115 F. Supp. 3d 1184, 1193 (W.D. Wash. 2015)

¹²¹ Magnesium Machine, LLC v. Terves, LLC, Case No. 20-3779 (6th Cir. Dec. 10, 2020)

¹²² In re PrairieSmarts LLC, 421 S.W.3d 296, 307 (Tex. App. 2014)

¹²³ 前記「営業秘密事件の審理と措置」参照

幾つかの州では、裁判例を踏まえると、営業秘密の侵害の事実が認定された際には、反証は可能であるもの、差止命令の要件である「取り返しのつかない（回復不可能な）損害の発生」という要件を充足すると推定される¹²⁴。例えば、イリノイ州の連邦地裁は、DTSA とイリノイ営業秘密保護法の事件で、反証可能な推定を適用した¹²⁵。オハイオ州や、カリフォルニア州の判決にも、同様のものがみられる¹²⁶。

これに対して、他の多くの州で、反証可能な推定を適用しないとするものが見られる¹²⁷。

(2) 金銭的賠償

米国の不法行為の損害賠償の一般規則に従い、損害賠償は、違反行為と事後的因果関係のある、かつ、相当因果関係のある損害に関してのみ認められる。そして、侵害行為がなければ、原告が有していたであろう元の地位に回復するのに必要な程度で付与される。

実際の事件で、営業秘密の侵害による損害を立証するのは容易ではないことが多い¹²⁸。この相当因果関係の立証の困難性を明確に示した判決が、連邦第 9 巡回控訴裁判所により下された

¹²⁹。

原告は、営業秘密の不正使用と不当利得を理由に、元従業員とその新雇用主である被告会社に対して訴訟を起こしたが、地方裁判所は、被告らの申立てに基づき、請求を却下する略式判決を下した。第 9 巡回区控訴裁判所はこれを認容した。

営業秘密の不正使用に基づいた、被告に対する損害賠償の請求について、裁判所は、まず、原告が主張する、営業秘密の不正取得、使用が十分に立証されていないと指摘した。その上で、営業秘密の喪失により、1,600 万ドルを超える価値をもつ営業秘密の損害が原告に生じているので、同額の賠償が発生しているとする専門家の報告書は、被告が侵害した事実を前提としており、採用できないと結論づけた。

¹²⁴ Brightview Grp., LP v. Teeters, 441 F. Supp. 3d 115, 138 (D. Md. 2020)

¹²⁵ Vendavo, Inc. v. Long, 397 F. Supp. 3d 1115, 1143-44 (N.D. Ill. 2019)

¹²⁶ Allied Erecting & Dismantling Co. v. Genesis Equip. & Mfg., Inc., No. 4:06CF114, 2010 WL 3370286, at *2 (N.D. Ohio Aug. 26, 2010)

¹²⁷ 例えば、DTSA に基づく営業秘密侵害事件で、連邦第 10 巡回控訴裁判所は、DTSA は、差止命令を許可するだけであり、強いるものではないと、結論した。First W. Capital Mgmt. Co. v. Malamed, 874 F.3d 1136, 1142-44 (10th Cir. 2017) 連邦第 3 巡回控訴裁判所も、今後起きる可能性がある開示行為は、差し止められるべき対象だが、既に開示された情報を差し止める必要がないとして、差止命令の付与を否定した。Campbell Soup Co. v. ConAgra, Inc., 977 F.2d 86, 91-93 (3d Cir. 1992)

¹²⁸ T-Mobile USA, Inc. v. Huawei Device USA, Inc., 115 F. Supp. 3d 1184, 1193 (W.D. Wash. 2015)

¹²⁹ Joshua David Mellberg LLC v. Will, No. 20-16215, 2021 WL 4480840, at *1 (9th Cir. Sept. 30, 2021)

裁判所は、原告の不当利得の請求についても、地方裁判所の判断を是認した。原告が、営業秘密の開発に数百万ドルを費やしたと主張し、財務書類を開示し、証言も提出したが、裁判所は、提出された証言を「一般者の意見」および「一般的な主張」として、判断の参考にしなかった。裁判所は、不当利得の理論に関して、原告が開発費に関する宣誓書を補足として提出したことについて、時期に遅れたものとして排除した。そこで、損害額計算を必要とする、連邦民事訴訟規則 26a(1)(A)(iii)を満たさなかったと認定した。

営業秘密保有者は、損害の立証をする代わりに、侵害者によって得られた利益の引渡し、ライセンスした場合に支払われるべきロイヤルティの支払いを求めることもできるので、合理的ロイヤルティの率が入手可能であれば、資料を提出することができる。

UTSA も DTSA も、懲罰的損害賠償を採用し、侵害行為が故意か過失かによって額を増加させることができる。

DTSA は、裁判所が、営業秘密侵害の訴えを濫用的に起こした原告、差止命令取消しを正当な理由なく求めた被告、意図的で故意に営業秘密を侵害した被告に対し、弁護士費用を負担させようとしており、原告としても、不合理な請求をすることはできない。

5 内部告発と営業秘密の使用・開示

前記の通り、DTSA は、一定の内部告発行為を、適正な営業秘密の使用であるとして、違法な侵害行為から除外する。この規定に関して、連邦オハイオ州地方裁判所は、正当な公益目的の営業秘密開示を免責する点に着目し、免責規定の適用を緩やかに認めた¹³⁰。

問題となった従業員は、その代理人を通じて、会社の違法行為を告発するために、営業秘密を開示したのであり、(1)情報使用の意図が違法行為の内部告発の目的「だけ」と考えても良いこと、(2)多少、自己の職責を超えて、会社の情報にアクセスしたとしても、その営業秘密へのアクセスだけを、営業秘密の使用から切り離して捉えて、不正であったとすることは、立法の目的、文言に反していることを理由として、従業員の主張を採用した。そこで、従業員の営業秘密開示は、情報のアクセスと一体として捉えられ、免責された。

第5章 準拠法・域外適用

1 判例法での準拠法

営業秘密侵害に関して、海外で不正に取得された米国法人の営業秘密の侵害には、特に保

¹³⁰ FirstEnergy Corp. v. Pircio, 524 F.Supp.3d 732

護法益と関連のある州の判例が適用されてきた。幾つかの州は、侵害行為が行われた地域、又は、被告が侵害行為による利益を受けた地域の法律を適用するとしているため、侵害行為がカリフォルニア州で行われる場合の他にも、侵害行為による利益を受ける地域が米国カリフォルニア州であれば、取得行為や使用行為が国外であっても、カリフォルニア州法が適用となる¹³¹。

また、多数の州で、原告の本店所在地の法律を適用する¹³²。したがって、米国テキサス法人の保有する営業秘密の侵害では、被告の営業秘密の取得行為、又は開示行為が国外でなされても、テキサス法の適用となる。このように記載すると、判例法では、無制限な適用があったかのように思われてしまうが、実際には、「不正な」使用、開示、取得に限定されており、原告あるいは被告に関係が深い州の法を適用した。あるいは、侵害品は、州に持ち込まれて、宣伝や販売の促進に使われていた事実がみられる事件が殆どであった¹³³。

2 侵害品の輸入と米国関税法の適用

関税法は連邦法であり、域外適用の問題が生じる¹³⁴。営業秘密侵害品が米国内に輸入されることになると、関税法第 337 条に基づいて、輸入についての不公正な競争手段、又は、不正な行為に対する ITC による調査と決定がなされ得る。その場合、ITC は、営業秘密の不正使用の調査の過程で、国内市場での不公正な競争から生じる不利益から国内産業を保護する必要がある限り、中国でなされる行為にも、調査と検討を加えることができるとされる¹³⁵。

3 DTSA 下の侵害行為と域外適用

イリノイ州の連邦地方裁判所は、被告である海外法人が、第三者により不正に取得された

¹³¹ カリフォルニア州法の営業秘密について、不正な開示を州内で存在したことを根拠に適用する判例に *Meggitt (San Juan Capistrano), Inc. v. Yongzhong*, No. SACV130239DOCMLGX, 2013 WL 12120067, at *2 (C.D. Cal. Sept. 26, 2013), *aff'd in part, dismissed in part sub nom. Meggitt San Juan Capistrano, Inc. v. Yongzhong*, 575 F. App'x 801 (9th Cir. 2014)、被告の活動中心の州で、被告が不正な利益を受けることを根拠に、被告拠点地法の適用があると示唆する判例に *Mergenthaler Linotype Co. v. Leonard Storch Enterprises, Inc.*, 66 Ill.App.3d 789, 23 Ill.Dec. 352, 383 N.E.2d 1379, 1389–90 (1978); *Goldberg v. Medtronic, Inc.*, 686 F.2d 1219, 1225 (7th Cir.1982); *Smith v. Dravo Corp.*, 203 F.2d 369, 373 (7th Cir.1953); *SIL–FLO, Inc. v. SFHC, Inc.*, 917 F.2d 1507, 1511–12 (10th Cir.1990).

¹³² *FMC Corp. v. Capital Cities/ABC, Inc.*, 915 F.2d 300, 302 (7th Cir.1990); *Restatement (Second) Conflict of Laws § 145, comment e* (1971).

¹³³ 原告と、（被告や、被告に営業秘密を漏洩した者が）積極的に契約関係に入っていたことが原因となっている場合など、州と接点がないとは言えない事情があった。 *Salton, Inc. v. Philips Domestic Appliances & Pers. Care B.V.*, 391 F.3d 871, 877–80 (7th Cir. 2004)

¹³⁴ See *WesternGeco LLC v. ION Geophysical Corp.*, 138 S. Ct. 2129, 2135 (2018)

¹³⁵ *TianRui Group Co. Ltd. v. International Trade Commission*, 661 F.3d 1322 (Fed. Cir. 2011)

営業秘密を海外で使用している場合に、侵害行為は海外なので、DTSA の適用はないと被告が主張したのに対し、侵害品が米国内に持ち込まれて、展示や見本として使用されている以上、米国内の「不正な使用」があると考えられ、域外適用の問題は生じない可能性があることを述べた¹³⁶。したがって、域外適用の問題が本当に生じるのかも検討する必要がある。

DTSA は、以下の場合に、米国外行為にも DTSA が適用されることを規定する¹³⁷。

- a. 侵害者が、米国の市民、若しくは、永住外国人である自然人、又は、米国、州若しくはその政治的区分の法律下で、組織された団体である。
- b. 米国で犯罪を達成させる行為が行われた。

イリノイ州の地方裁判所により、明文による域外適用は重要であるが、それだけでなく、「米国内の」不正な使用が緩やかに決定される可能性が示された¹³⁸。

第 6 章 営業秘密侵害の事件数

1 訴訟数の概観

2017 年以降、およそ年間 1,300 件ほどの営業秘密侵害事件が提起されている。ことに、営業秘密侵害事件の連邦裁判所への提起は、DTSA 判例の誕生した 2016 年から 2017 年に 30% 増加し、その後は特に増減がない¹³⁹。

2020 年の営業秘密侵害事件の 72.9%、2019 年の営業秘密侵害事件の 72.5% で、DTSA に基づいた請求が含まれていた。

営業秘密の訴訟が頻繁に提起される裁判地としては、以下の州がある：

- カリフォルニア州；
- イリノイ州；
- ニューヨーク州

2 訴訟結果

2017 年から 2020 年の間での事件の終局は下記のとおりであった。

- 67% の事件は、本案に関する判決前に和解
- 74% の本案終局判決に至った事件で、恒久的差止命令を発令

¹³⁶ Philips Med. Sys. (Cleveland), Inc. v. Buan, No. 19-CV-02648, 2021 WL 3187709, at *10 (N.D. Ill. July 28, 2021)

¹³⁷ 18 U.S.C. § 1837

¹³⁸ Motorola Sols., Inc. v. Hytera Commc'ns Corp., 436 F. Supp. 3d 1150, 1162 (N.D. Ill. 2020)

¹³⁹ LexMachina 調査結果。この結果には、DTSA に基づく請求、UTSA（州法）に基づく請求、刑事訴追、行政的措置のすべてが含まれる。

- 54% の本案終局判決に至った事件で、暫定的差止命令を発令
- 65% の本案終局判決に至った事件で、一時的抑止命令を発令

全体で、12 億 9400 万ドルの金銭的賠償が認められた（2020 年一年では、5 億 4100 万ドル）。これには、以下を含む：

- 現実の損失；
- 懲罰的賠償；
- 合理的ロイヤルティ
- その他の損害；
- 判決前の利息；
- 弁護士費用

2019 年と比較して、裁判所は、2020 年の一年で、営業秘密事件一件あたりで、より高額の金銭的賠償を認めた。

3 解決の期間

2017 年から 2020 年の間での事件解決に要した平均時間：

- 略式判決まで： 617 日
- 審判まで： 795 日
- その他： 259 日（和解を含む）

4 連邦経済スパイ法

米国司法省（DOJ）は、外国人又は外国法人による営業秘密侵害事件の捜査、対中国の経済スパイ法事件の訴追を主に手掛けてきた機関である。DOJ が扱った事件としては、非常に大幅なコンピューターシステムへの侵入、および、営業秘密の不正取得に対する外国の軍関係者の起訴、外国の政府及び外国の企業に代わって営業秘密の不正取得を敢行した個人及び企業体の起訴、並びに、多数の外国人による営業秘密の窃取事例の訴追がある¹⁴⁰。

18 U.S.C. § 1831（スパイ目的による営業秘密の侵害行為を刑事処罰する規定）が、裁判所の意見（中間的判断含む）で引用された事件は、同法が制定された 1996 年以降全 188 件あり、2021 年 11 月 27 日までの 5 年間で 129 件、2021 年 11 月 27 日までの 3 年間で 80 件であった。他方、18 U.S.C. § 1832（非スパイ目的による営業秘密の侵害行為を刑事処罰する規定）が、裁判所の意見（中間的判断含む）で引用された事件は、1996 年以降全 282 件であり、2021 年 11

¹⁴⁰ 米国司法省, Report to Congress Pursuant to the Defend Trade Secrets Act <https://www.justice.gov/criminal-ccips/page/file/1101901/download> (最終アクセス日 2022 年 2 月 18 日).

月 27 日までの 5 年間で 142 件、2021 年 11 月 27 日までの 3 年間で 86 件であった。このことから、同法違反として事件となる刑事事件又は民事事件は、特にこの 3 年間で増加していると理解される。

FBI の年間報告によると、連邦経済スパイ法の立件数は、ここ数年で増加している。（括弧内は、年間知財犯罪件数中の割合）

- 2019 Economic Espionage Act Economic espionage, 18 U.S.C. § 1831 2 (3%)
Theft of trade secrets, 18 U.S.C. § 1832 14 (22%)
- 2018 Economic Espionage Act Economic espionage, 18 U.S.C. § 1831 1 (2%)
Theft of trade secrets, 18 U.S.C. § 1832 10 (14.7%)
- 2017 Economic Espionage Act Economic espionage, 18 U.S.C. § 1831 2 (3%)
Theft of trade secrets, 18 U.S.C. § 1832 9 (11%)
- 2016 Economic Espionage Act Economic espionage, 18 U.S.C. § 1831 1 (1%)
Theft of trade secrets, 18 U.S.C. § 1832 5 (6%)

第 7 章 営業秘密関連の法改正の動き

1 営業秘密法

DTSA 成立以来、連邦法の改正は現在までなされていない。2021 年春には、米国の核心的技術に関わる技術に関して、外国人による営業秘密の侵害を覚知した場合に、省庁間での連絡を確立し、関税、輸入、証券・金融取引、知的財産保護等に対する制裁を加えることを可能とする法案が、上院議員の Graham Lindsey 氏により提案された¹⁴¹。

州営業秘密法の改正の動向は、発表がない。

2 サイバーセキュリティ政策

前政権から重点が置かれている、対中国対策、サイバー犯罪による国家機密情報の漏洩対策については、規制が引き続き強化されている。

(1) 輸出規制

2021 年 10 月 21 日、米国商務省産業安全保障局は、重要な暫定最終規則（暫定規則）を発表した¹⁴²。暫定規則は、サイバーセキュリティとランサムウェアの問題に対する、政府全

¹⁴¹ 「中国による営業秘密盗取との戦闘法」と第する法案を提案しているが、進行がみられない。S1245-CCP Trade Secrets Act, <https://www.congress.gov/bill/117th-congress/senate-bill/1245/text>.

¹⁴² 米国商務省、商務省は、民間人の監視およびその他悪意のあるサイバー活動で使用する品目の輸出管理を強化（最終アクセス日 2022 年 2 月 28 日）
<https://www.commerce.gov/news/press-releases/2021/10/commerce-tightens-export-controls-items-used-surveillance-private>.

体の重点化を反映し、悪意のあるサイバー活動に使用できる、侵入ソフトウェア、ネットワーク監視機器、及び、関連技術などの「サイバーセキュリティアイテム」の新しい輸出管理を確立する。この規則には、新しい輸出管理分類番号、新しく定義された用語、及び新ライセンス例外「輸出許可されたサイバーセキュリティ」（ライセンス例外 Ace）が組み込まれている。パブリックコメントに基づいて、変更が加えられなければ、2022 年 1 月 19 日（公開から 90 日以内）に発効する予定である。

暫定規則は、「正当なサイバーセキュリティ活動」を妨げないように「適切に調整」されることを目的とする。しかし、国グループ D の国（中華人民共和国など）のユーザーとビジネスを行う、サイバーセキュリティ分野で事業を行っている企業は、サイバーセキュリティアイテムのエンドユーザーが、「政府のエンドユーザー」か「非政府のエンドユーザー」であるか、評価が必要になる。前者では、ライセンス例外 Ace が利用不可能である。提案された新しいフレームワークでは、追加のデューデリジェンスが必要になりうることに注意すべきである。

(2) 5G 等の通信環境

2021 年 11 月 11 日、バイデン大統領は、2021 年安全設備法に署名した¹⁴³。これにより、連邦通信委員会は、同委員会の「対象リスト」に記載の機器及びサービスについて、以後は承認を審査しないか、又は、承認しないことを明確にしなければならなくなった。2021 年 3 月 12 日に最初に公開されたリストには、米国政府が以前、国家安全保障上のリスクとして特定した、中国の電気通信、及び、セキュリティカメラ会社が含まれている。既存の制限は、政府の調達と、助成金の文脈で、そのような指定項目の採用を制限する。安全設備法は、これに加え、連邦通信委員会に、米国内の誰もが、特定の中国の技術を使用することを禁止する規則を制定するように促すものであり、著しい効果の増加が予定される。

現在、対象リストには、(1)Huawei Technologies 社、(2) ZTE Corporation、(3) Hytera Communications Corporation、(4) Hangzhou Hikvision Digital Technology Company、(5) Dahua Technology Company、及び、それらの子会社や関連会社が含まれている。

(3) 通商法第 301 条による調査

トランプ大統領は、2017 年に改正された 1974 年通商法（貿易法）の第 301 条に基づく、

¹⁴³ ホワイトハウス、法案へ署名：H.R.3919（Nov. 11, 2021）
<https://www.whitehouse.gov/briefing-room/statements-releases/2021/11/11/bill-signed-h-r-3919/#:~:text=signed%20into%20law%3A-,H.R.,unacceptable%20risk%20to%20national%20security.>

中国による不正な貿易慣行に関する調査を行うよう命じた¹⁴⁴。第 301 条は、潜在的に対応可能な外国の行為、方針、又は、慣行の、以下の 3 つのカテゴリーを定めている。

- i. 貿易協定違反
- ii. 不当（米国の国際的な法的権利と矛盾するもの）で、米国の商取引に負担をかける、又は、制限する行為、ポリシー若しくは慣行
- iii. 不合理又は差別的であり、米国商取引に負担をかけたり、制限したりする行為、方針、又は慣行。

このうち、第 3 のカテゴリーの行為が、2017 年の調査に最も関連していた。

調査の結果、中国は、合併事業の要件、外国投資の制限及び行政審査とライセンス供与のプロセスを使用して、米国企業からの技術移転を要求又は圧力をかけており、米国企業からのライセンス供与やその他の技術関連の交渉において、市場ベースの条件を設定する能力を奪っていること、加えて、中国は、大規模な技術移転を生み出すために、米国の企業や資産へ、体系的な投資と買収を指示し、不当に促進していると結論づけた。そして、USTR は、2018 年 7 月から、対中国向けの 25% の従価税を行うことと決定した。

導入された中国物品に対する追加関税賦課は、除外の申請の許可を受けることができれば、これを免れることができるようになっていたが、2020 年末に失効した¹⁴⁵。バイデン政権は、国内製造業の部品不足等の状況を踏まえ、2021 年 10 月に、一度失効した除外を復活させる予定であると公表しており、今後、除外の復活が見込まれている。

第 8 章 国際協力・他国との連携状況

前述のとおり、経済スパイ法は、域外適用規定を設けるなど、米国捜査・訴追機関が、国際的な営業秘密事件で、幅広く管轄権を掌握することを目指すものと理解されるが、実際には、対人管轄、事物管轄から、捜査・訴追権限には、地理的な制限がある。海外に所在する外国人が、海外に位置している間に行った行為に関しては、米国の捜査機関、司法機関の権能は限定あるいは否定されてしまうのが通常で、更に、関連する営業秘密が米国内にない場

¹⁴⁴ 同条は、貿易相手のさまざまな不公正な行為、政策、慣行に対処するために使用できる、米国の主要な規制手段である。USTR, 974 年通商法第 301 条に基づく技術移転、知的財産、およびイノベーションに関連する中国の行為、方針、および慣行に関する調査の結果（March 22, 2018）

¹⁴⁵ USTR, USTR は、第 301 条の関税の対象となる中国製品の潜在的除外について、コロナウィルス関係の物品については、除外の復活を 11 月に決定した。米国 USTR、「製品除外の延長に関する通知：技術移転、知的財産、およびイノベーションに関連する中国の法律、方針、および慣行」86 Fed. Reg. 63438 (2021 年 11 月 16 日)<https://ustr.gov/about-us/policy-offices/press-office/press-releases/2021/october/ustr-requests-comments-reinstatement-targeted-potential-exclusions-products-china-subject-section>.

合、管轄が否定されかねない¹⁴⁶。

しかし、経済スパイ法は、（1）犯罪者が、米国市民あるいは永住外国人である、若しくは、米国法に基づいて組織された法人である、営業秘密の侵害、又は、（2）犯罪を達成させる行為が米国内で行われているものに、米国の捜査機関に管轄権を与える¹⁴⁷。

DOJ の Computer Crime and Intellectual Property Section (CCIPS), Office of International Affairs in the Criminal Division (OIA) が、これまでに DOJ が訴追した国際的営業秘密事件の捜査を手掛けてきた¹⁴⁸。CCIPS はサイバーラボというグループを有し、ハッキングを伴うコンピューター利用による侵害で、証拠の収集、解析を行うことができる。

犯人が米国内にいない場合などは、海外の捜査機関・司法機関から協力を得て事件を捜査・訴追することが重要となる。DOJ 内のリソースだけでなく、海外の捜査機関に対して、捜査協力を求める場合、米国が外国と締結している刑事共助条約を通じて、犯人の搜索、証拠収集の要請がなされる。例えば、証人の召喚、証拠の提出、搜索令状の発行に関する権限を米国検察官に与えるものであるが、実際に権限を行使するためには現地の捜査機関の執行が不可欠となる。

これに加えて、広域な組織的犯罪の場合には、インターポール、ユーロポールを通じて国際犯罪への捜査協力を、複数国に申請することがなされる。

米国の連邦捜査局（FBI）は、世界中の法執行機関、諜報機関、および、セキュリティサービスとの関係を構築しており、自国民や自国企業を保護するために、特別捜査官やその他の要員を 63 の海外支所に配置している¹⁴⁹。したがって、海外拠点を通して、迅速かつ継続的な情報交換が可能となっている。FBI は、捜査対象に、組織的犯罪、サイバー犯罪（サイバー部門が担当する）を含むため、知的財産権事件や営業秘密侵害事件（民間企業の事件は、犯罪捜査部門の知的財産権プログラムが扱う）も、捜査を行うことができる。

米国は、TRIPS 協定に基づいた知的財産権保護制度の強化を WTO に訴えるなどして、他国に要求してきた。また、USTR は、ASEAN 諸国に対しても、かねてより、国際的な知的財産権保護の協調について、合意・協定の交渉を重ねてきた。例えば、2016 年 11 月には、ペルーのリマで開催されたアジア太平洋経済協力（APEC）の指導者と大臣による、「営業秘密の保護と侵害に対する執行の最善の慣行」の合意に至った¹⁵⁰。

¹⁴⁶ 上記「準拠法・域外適用」を参照。

¹⁴⁷ 上記「準拠法・域外適用」を参照。

¹⁴⁸ 米国司法省、脚注 140

¹⁴⁹ FBI、海外支所（最終アクセス日 2022 年 2 月 18 日）<https://www.fbi.gov/contact-us/legal-attache-offices>.

¹⁵⁰ 営業秘密の保護と侵害に対する執行の最善の慣行(2016)

第9章 仲裁の利用

上記のとおり、営業秘密侵害事件における、比較的多額の認容額、高率の恒久的差止命令は、裁判所における訴訟を選択する、極めて重要な動機となっている。

しかし、裁判所における審理では、少なくとも、営業秘密の内容や、自社の技術の内容について主張、立証しなければならず、措置をとらない限り公開されてしまう結果となり、自社の機密情報を、競争相手に知られて（推察されて）しまいかねない。また、カリフォルニア州では、原告が、訴えの最初から、合理的な特定性をもって営業秘密を特定しなければならないという要求が存在する。

これに対して、仲裁手続では、仲裁自体の存在も秘密にでき、パブリシティの悪影響を防ぎえるうえ、仲裁手続で交わされた当事者の主張、提出された証拠について、より秘密性が確保される。したがって、営業秘密の侵害事件を、裁判を介さず、仲裁手続で解決することは、当事者にとって有益な場合が多くある。それに、裁判手続は、長期に及び、費用も多額となりやすい。

一般商事件での仲裁手続利用が定着してきた米国では、営業秘密事件の仲裁手続の利用も、珍しいことではないとされる¹⁵¹。

第10章 ライセンス、生産委託、合併会社設立で気をつけるべきポイント

第一に、営業秘密には、「当該状況下で、秘密性を保持するための合理的な措置がとられている」ことが要件とされているため、機密情報や営業秘密を、秘密保持義務への合意のないまま、第三者に提供することは、それらの「機密性」を失わせる結果となりかねない¹⁵²。

次に、営業秘密の合理的な特定性が、州法上要求されるのと同様に、契約においても、何が営業秘密か、当事者にとって明確であるように定義する必要がある。法律関係を明確化し、将来の紛争を防ぐためにも、秘密保持義務（守秘義務）を明文で盛り込むのが賢明であり、必要性が高い。

ライセンスを受けるなどして、機密情報あるいは営業秘密を保持する者が、「秘密性を保持するための合理的な措置」を取っているか否かは、以後の営業秘密の保護に重要な事実として関わってくる¹⁵³。このため、秘密保持義務の内容を秘密保持契約書内に盛り込むことが重要であると推奨される。

¹⁵¹ Jeremy Cohen, et al., Preparing for Trade Secret and Restrictive Covenant Litigation While the Court Near You is Closed, Seyfarth Shaw (Apr. 14, 2020) <https://www.jdsupra.com/legalnews/preparing-for-trade-secret-and-40528/>.

¹⁵² 第1章「営業秘密の定義」を参照

¹⁵³ UTSA 第1条、18 U.S.C. § 1839(3).

裁判所の述べたように、

- 自社あるいはライセンシーの従業員が、自己の情報通信機器を使用できないようにするか、それを許す場合は、アクセスと使用のコントロールのための厳格な制限を課すこと、
- パスワードによる保護なく、コンピューターのアクセスや、ファイルを保存や読み出しすることができないこと、
- ライセンシーにおいて、機密情報、営業秘密を、機密性に関する程度でラベルすること、
- ライセンシー従業員の機密性保持の言明、
- 情報が、業務を実行するため少なくとも潜在的にアクセスを必要とする人へのみ開示されている（「知る必要があるベース」）、
- 情報の開示を受ける者は、秘密保持義務に拘束され、情報に関して、この秘密保持義務を負っていることを認識していることの確認

は、プラスの要素となるため、含めることが推奨される¹⁵⁴。

本報告書に添付の書式は、こうした重要な要素を含んだ保護措置が取られるように、ライセンシーに義務付けている。ライセンシーの中の誰が機密情報に触れうるかについての特定は、添付文書の形で行われるのが現実的と考えられる。また、相手会社の機密情報を取り扱う者と個別に、同様の秘密保持契約を締結することも勧められる。

ライセンス、生産委託、合併会社設立の際に、当事者間で契約書がかわされる場合、契約書に機密保持条項を盛り込むのは通常なされるが、米国法が準拠法である場合には、以下の問題が起こりうるので注意し、米国弁護士に相談することが推奨される。

1 ライセンス契約

(1) 機密情報、営業秘密の特定

あまりに広範囲で網羅的な条項は、機密性保持の実施が困難であり、実務的ではない。あまりに秘密保持義務が広範な契約は、無効とされたり、法的拘束力を否定されることもある。また、雇用関係に関連する場合は、被用者の労働の自由が考慮される。

実際には、情報の機密性のラベルが有意義と考えられる。機密情報とすべき必要性があること、実際に機密情報として扱われていることが、後に立証できるよう確認すべきである。

一方、相手会社が、機密情報や営業秘密を利用して生み出すデータや情報を、機密情報や営業秘密に含めることは、多くの場合に、不可能ではないと考えられる。

¹⁵⁴ 第1章「営業秘密の定義」を参照

(2) 機密情報、営業秘密へのアクセス、使用目的、使用方法の限定

契約条項を作成する場合、何が許されるか、そして、何が不正取得、使用、又は、開示になるかを明確にすることは、ライセンシー及びライセンサーの利益を守り、また、有効な関係を維持するためにも大切である。例えば、ライセンシー側で、パスワード等アクセス制限を設定すること、アクセスできる者を一定の被用者、関係会社の被用者、専門家、監査人等に制限すること、アクセスの目的と使用方法を制限することなどが、考えられる。

侵害行為者が、営業秘密の不正使用、開示、取得にあたる事実を認識していたことや、認識すべきであったことが、営業秘密侵害の前提とされており、許可事項と不許可事項を分別することが意味を持つと考えられる。

営業秘密保有者において、機密性を保つ合理的な措置をとっていたかに関連して、電子機器使用時のパスワード要求、不用意な紙媒体での処理のないことは必須と考えられる。

(3) 契約終了後の情報の返却あるいはデータ削除義務

秘密保持義務の内容として、提供された機密情報や営業秘密は、契約関係終了時に保有者に返却すること、また、バックアップも含めて、保存されたデータから削除するように要求すること、それを確認することを明記することが必要である。これは、前記の、機密性を保つ合理的な措置の認定にも、プラスの要素として働くと考えられる。

(4) 補償条項

相手方の秘密保持義務違反の結果生じた損害について、相手方に補償の義務を負わせることは、多くの場合に行われている。秘密保持義務条項の有効性が認められる場合、こうした補償条項の効力も同様に認められるであろう。

(5) 損害額

機密情報・営業秘密保有者は、不正取得、使用、あるいは、開示により生じた損害に対する賠償として、特約がない場合、自分の被った損害を立証して、その填補を求めることができる。この損害の立証は困難となることも考えられるので、損害額の算定について、事前に合意しておくことも考えられる。

(6) 仲裁合意

裁判による紛争解決と比較し、仲裁は、営業秘密、機密情報の保護に適し、手続きで提出あるいは開示された情報の秘密性が保たれやすいと考えられている。そこで、ライセンス契約にあたって、仲裁条項を挿入して、仲裁により契約の紛争を解決し、ライセンサーの機密情報や営業秘密の保護を図ることは、積極的に検討されるべきである。

2 生産委託契約

上記に列挙した注意点は、生産委託契約にも当てはまる。委託者としては、受託者の生産ラ

インの運営状況、生産品の数量等の確認体制、保存・管理状況を十分確認することが、特に重要となると考えられる。そこで、契約書にも、これらの事項について、受託者に報告、保証、あるいは誓約をするよう義務づけることは検討されるべきである。

生産委託契約では、受託者が、第三者の機密情報、営業秘密情報をたまたま持っていて、委託者の製品の製造に使用してしまった場合、第三者から、機密情報・営業秘密の不正使用、開示にあたるとして、請求を起こされてしまう可能性がある。委託者自身が知り得ない場合、委託者に対する請求は成功しないとしても、暫定措置により、生産に対する影響が起こりうる。そこで、生産された製品が、受託者と取引関係のある、他社の機密情報・営業秘密の侵害をしないことを誓約する保証を要求することは、検討されるべきである。

機密情報、営業秘密へのアクセス、使用目的、使用方法の限定に関して、受託者から第三者への再委託を禁止することも考慮すべきである。

3 合併契約

合併会社は、参加当事者が提供した、あるいは、合併会社自身が調達した人材、技術、データ、施設、及び、資材を使用して事業を行うことが多い。参加者の様々な機密情報、営業秘密が提供されることもある。したがって、合併会社が研究や開発をして得られる成果物に対して、どの者に所有権あるいは管理権が帰属するのかを契約で明確化しておくことは、特に重要となる。

欧州

第1章 営業秘密の定義

1 EU指令の制定と主要加盟国の国内法移行

2016年、欧州連合で制定された「非開示のノウハウ及び事業上の情報（営業秘密）の違法な取得、使用、開示に対する保護に関する指令（EU）2016/943」（以下「EU指令」という。）は、事業に関して利用されている価値ある情報が、競争相手に盗用されたり、無断で使用、あるいは、開示されてしまうことにより、企業や個人主が築いた市場競争力を奪取されてしまう事態が起こらないように、不公正な競争を防ぐ観点で、各加盟国で制定されている法律を強化し、調和させることを目的とした、法的文書である。EU指令自体には、直接的に対私人的な法的効力を及ぼすものでないものの、各加盟国は、2018年6月9日までに、EU指令を国内法に移行する措置をとる義務を負った。その結果、第3章「営業秘密侵害に関連する法律、規制の概要」で説明するように、各加盟国で国内法制定が実現している。

EU指令は、営業秘密の違法な取得、使用、開示に対し、民事上の救済を規定するとともに、刑事制裁、行政措置、公共調達、その他の政府・公共機関での国内手続きにおける営業秘密の使用に関しては、EU加盟国の国内法に委ねられている。EU指令以外に、EU内市場における、企業による消費者への不公正な商慣行に関する指令が存在し¹⁵⁵、不公正な競争に対して、不公正商慣習指令が、EU指令に加えて適用される場合がある。

2 EU指令による「営業秘密」の定義

EU指令の第2条によると、「営業秘密」とは次のような情報を意味する¹⁵⁶。これは、知的所有権の貿易関連の側面に関する協定（TRIPS協定）に含まれる定義に基づいており、米国や日本で一般に受け入れられている「営業秘密」の概念と、定義上は、ほぼ等しいものとなった

¹⁵⁷。

（1）第2条の規定内容

営業秘密の定義は、ノウハウ、ビジネス、及び技術情報を網羅するように解釈されるべき

¹⁵⁵ 2005/29 / EC（不公正商慣習指令）

¹⁵⁶ EU指令第2条

¹⁵⁷ 世界貿易機関の知的所有権の貿易関連側面に関する協定（1994年4月15日）第39条の定義規定。EU指令は、世界貿易機関（WTO）加盟国が遵守すべき、TRIPSによる統一された定義に従い、それを欧州連合に正式に導入したものである。

とされ、それらの秘密性を保持することに、正当な利益があり、秘密として保持されることが期待されるものを意味する¹⁵⁸。これにより、従業員が、通常の雇用過程で得られた経験やスキルだけでなく、業界内部者が、各自容易に作成することが可能な情報も、定義から除外されることが予想される。

- a. 単体として、又は、そのコンポーネントの正確な構成と組み立てにおいて、その種の情報を扱う業界内関係者の間で、通常、一般に知られておらず、又は、容易にアクセスできない、という意味で秘密である。
- b. それが秘密であることから、商業的価値がある。
- c. 情報を秘密に保つために、合法的に情報を管理している者によって、当該状況下で、合理的な措置が講じられている。

EU 指令では、具体的にどの程度の秘密性保持のための措置が「合理的」とみなされるか、及び、どのような状況下で、問題となった情報が「容易にアクセスできない」情報であるかについて、特別な規定が置かれていない。今後、これらの用語の解釈（殊に、秘密性保持の措置の要求）に関し、各加盟国の国内法の規定や判例法により、解釈のばらつきが生じうる。

上記の要件のうち、秘密性のために「商業的価値がある」について、実際の金銭的な価値には限定されておらず、潜在的に有益なものであれば、要件は満たされると捉えられる¹⁵⁹。例えば、保有者により営業秘密として扱われ、実際に開示が厳しく制限されてきた情報は、反証が無い限り、商業的価値があると見なされるべき、とするアプローチは、EU 指令によって排斥されていない。また、保有者が受ける利益は、科学的新規性、技術的優越性だけでなく、ビジネス的効率性、経済的有利性、戦略的優越性、競争力が含まれるため、保有者の債務額や財務諸表に存する情報、顧客のクレジットカード情報も含まれる。

EU 指令第 2 条の解釈に争いが生じれば、最終的には、欧州連合司法裁判所（CJEU）が判断することになる。

(2) EU 指令による「保有者」の定義

EU 指令には、「保有者」とは、営業秘密を合法的に管理する自然人又は法人を意味すると規定されている¹⁶⁰。これには、営業秘密を発明した者のみならず、発明者の雇用主、関連会社、ライセンシーが含まれる。

(3) EU 指令による「侵害者」の定義

¹⁵⁸ EU 指令序文

¹⁵⁹ EU 指令序文

¹⁶⁰ EU 指令第 2 条

侵害者とは、営業秘密を、違法に取得、使用又は開示した自然人、若しくは、法人を意味する¹⁶¹。したがって、侵害者は必ずしも、営業秘密保有者と直接的な契約関係がある者や、事実上の競争、取引関係にある者に限られない。しかし、「違法に」との限定があることから、適用される法律で、取得、使用、又は開示が、違法と判断されることが前提となる。

(4) EU 指令による「侵害品」の定義

侵害品とは、違法に取得、使用、又は、開示された営業秘密に、相当に利益を受けるデザイン、機能、製造プロセス、マーケティング、又は、特性を持つ物品を言う、と定義している。侵害品と認定するには「相当に利益を受ける」ことが必要となるため、立証は容易ではない可能性が高い。更に、各加盟国の裁判所が異なった解釈をする可能性もあろう。

第 2 章 営業秘密侵害行為の定義

1 EU 指令における営業秘密侵害行為

(1) 第 3 条による侵害行為からの除外

EU 指令第 2 条は、上記の通り、侵害者とは、違法に営業秘密を取得、使用、若しくは、開示する者を言う、と定義し、侵害行為は、「違法に取得、使用、又は開示」することであることを明らかにしている。この点で、第 3 条は、「違法」ではない場合を例示的に列挙するが、これらの行為のうち最初の 2 つの類型は、他の国々でも、殆ど営業秘密侵害行為とはみなされていない¹⁶²。下記 c 及び d の類型は、管轄により違法とみなされている可能性がある。

- a. 独立した発見や創造
- b. 一般公衆が入手可能であった、若しくは、営業秘密の取得に法的制約を課されていなかった入手者が所持していた、製品や物品の観察、研究、解体、検査
- c. 連合法や法令、慣習に則った、情報及び諮問を得られる、労働者あるいは労働組合の権利の行使
- d. その他、行為時の状況下で、誠実な商慣習に合致した行動

(2) 第 4 条の規定

EU 指令は、更に、第 4 条において、どのような範囲の行為が、「違法な取得、使用、又は開示」に該当しうるか、行為者の保有者に対する関係、立場に応じて、具体的な侵害行為

¹⁶¹ EU 指令第 2 条

¹⁶² 日本でも、リバースエンジニア等で得られた情報、公開情報から察することができた情報については、不公正な競争とは言えず、営業秘密侵害とは考えられていない。

を例示的に列挙している¹⁶³。

① 営業秘密の取得者

営業秘密保有者の同意なく、以下のいずれかの行為を行った場合、侵害行為に該当する。

- a. 保有者の管理下にある、営業秘密を含んだ、若しくは、営業秘密を取り出しうる、文書、物件、材料、物質、又は、電子ファイルへのアクセス、使用、若しくは、コピー
- b. 行為時の状況下で、誠実な商慣習に反するその他の行動

前半部分は、同意なく営業秘密を含んだ有体物や無体物にアクセスする行為を、侵害行為とする。したがって、目的は必要でないことはもちろん、故意や過失を問わないように読める¹⁶⁴。

以上のように、EU 指令は、「誠実な商慣習に反する」行為という、漠然とした内容の行為を、営業秘密の違法な取得に含めている。例えば、営業秘密保有者の同意が欺罔により得られた場合、同意が撤回された、若しくは、効力を失ったことが明らかな場合には、「誠実な商慣習に反する」に該当すると考えられる。同じ定義を国内法に有する、加盟国の裁判例の今後の動向を注意する必要がある。

② 営業秘密の開示者、使用者

営業秘密保有者の同意なく、以下のいずれかの行為を行った場合、侵害行為に該当する。

- a. 営業秘密を違法に取得（上記(1)の規定にあたる行為）
- b. 秘密保持義務、又は、営業秘密を開示しない義務に違反
- c. 契約上の義務、又は、営業秘密の使用を制限すべき義務に違反

以上のように、営業秘密の違法な取得者以外にも、守秘義務を負う被用者、会社役員、アドバイザー、会社買収の交渉相手等、営業秘密の開示、使用に関して制限を受ける者も、開示や使用ができない。

③ 営業秘密の取得者、使用者、開示者

営業秘密が、違法に使用あるいは開示していた（上記②や本項にあたる行為）者から、直接的、若しくは、間接的に得られた事実を、認識していたか、その行為時の状況下で、認識すべきであった場合

④ 侵害品の製造者、提供者、市場展開者、輸出者、輸入者、若しくは保管者

¹⁶³ EU 指令第 4 条

¹⁶⁴ ICC, Protecting Trade Secrets-Recent EU and US Reforms (2019) 16, available at <https://iccwbo.org/publication/trade-secrets-report/>.

営業秘密が、違法に使用されていた（上記②、③にあたる行為）事実を、認識していたか、その行為時の状況下で、認識すべきであった場合

具体的にどのような行為が営業秘密侵害行為となるかは、各加盟国が国内移行で行う制定法の規定、及び、裁判所の解釈に依存することは否めず、実務上、相当な幅が生じるのではないかと考えられる¹⁶⁵。

2 営業秘密侵害行為に対する例外

EU 指令は、第一次的には、欧州連合内での営業秘密保護を強化するための原点として制定されたが、中には、情報のような無体物が財産として保護されてよいか、といった保護の拡大、強化に対する懸念も存在した¹⁶⁶。これに対し EU 指令は、営業秘密の定義において、「合理的」な秘密性保持措置を要求し、「違法性」についての限定する規定を盛り込んだほか、侵害行為に関し、下記のような例外規定を設けた。

- a. メディアの報道の自由、多様性を含む、表現、及び、情報の自由の権利行使
- b. 公共の利益を保護する目的での、違法行為、不正行為、又は不法行為の暴露
- c. 連合法や国内法に則った、組合代表の機能の正当な権利行使としてなされる、労働者から組合代表への開示で、必要があるもの
- d. 連合法や国内法に認められた正当な利益を保護する目的での行為

EU 指令は、比例性と濫用に関する保護措置に基づくだけでなく、内部告発や、第三者の犯罪や違法行為に関する情報提供を、営業秘密侵害から除外することで、保護を与えている¹⁶⁷。すなわち、「営業秘密」の定義には、違法又は不正な商慣行に関連する情報（例えば、過去の違反に関する情報で、規制省庁へ届け出ていないもの）も含まれてしまうところ、そのような情報は法的保護を与えるべき意義に乏しいと考えられ、また、公益を促進する、違法行為に関する通報が、不正行為を隠匿する事業主により妨げられるのは不合理である。そこで、EU 指令は、違法行為、不正行為、又は不法行為を明らかにする目的の例外規定を設け、開示を正当化することができることとした。

第3章 営業秘密侵害に関連する法律、規制の概要

1 EU 指令の国内法移行

例えば、ドイツの新しい営業秘密法は、最小調和の程度で、EU 指令を実施することを目的

¹⁶⁵ 過失、故意等の主観的要件、及び、転得者はどうか、等。

¹⁶⁶ EU 指令序文

¹⁶⁷ EU 指令第5条

として制定されたが、営業秘密の定義の変更を無理なくされた。その他、ドイツで強固に貫かれていた、訴訟手続の公開制度との関係から、営業秘密を公開から保護する手続について導入し、今後の知的財産権訴訟における、重要なステップとなることが期待される¹⁶⁸。

英国の新しい営業秘密法は、英国が欧州連合から脱退する前に制定され、EU 指令の立法目的を充足するような内容の規定となっている¹⁶⁹。特に、営業秘密の定義の面で、かつての営業秘密の概念を変更するものと予想される¹⁷⁰。一方、コモンローの下で発展した、従前より存在する機密情報に対する法的保護は、併存することが示唆され、新法下の保護に関し、今後の裁判例の展開が待たれるところである¹⁷¹。

フランスでは、商事法の中に、EU 指令を実施することを目的として条文が新設された¹⁷²。民事事件として、営業秘密所有者が、損害賠償請求、差止請求等を求めることができ¹⁷³、また、侵害者の悪質性の程度に応じて、損害額の増額がなされるように規定されている。但し、濫用的な訴訟を起こした原告に対しての制裁手段が置かれていることが、他に見られない特徴となっている¹⁷⁴。

チェコ共和国は、知的財産権の救済に関する 1 つの条項を修正するだけで EU 指令を移行した¹⁷⁵。

ポルトガルでは、営業秘密保有者は、情報を秘密に保つために必要なすべての措置を講じる必要があるとの規定となっている。これには、秘密性を維持するための合理的な措置を超えた措置が、必要になる可能性があると思われる。

このように、EU 指令自体は、営業秘密という財産権を取り出して、統一した定義を用意、確立し、欧州連合全体で均一な最低限の保護基準を確立したという点では重要であるが、各国間での法制度や保護の内容は異なったままである。すなわち、EU 加盟国は、EU 指令に定められた、特定の責任除外規定、及び、自由保障措置の遵守を条件として¹⁷⁶、より広範囲の営業秘密保護を提供できる。

¹⁶⁸ 本書「ドイツ」編

¹⁶⁹ Mr. Williams 氏インタビュー

¹⁷⁰ Mr. Williams 氏インタビュー

¹⁷¹ Mr. Williams 氏インタビュー；本書「英国」編を参照

¹⁷² フランス商事法第 L. 151-7 条

¹⁷³ 第 L. 152-3 条

¹⁷⁴ 第 L. 152-6 条

¹⁷⁵ Rogier de Vrey, EU: Trade Secret Law Reforms, CMS (最終アクセス日 2022 年 2 月 18 日) <https://cms.law/en/int/publication/eu-trade-secret-law-reforms>.

¹⁷⁶ EU 指令には、内部告発者の保護、表現の自由、雇用者の権利の保護に関する規定が設けられた。

2 営業秘密侵害に対する刑事処罰

(1) 刑事根拠法規

オーストリア、ベルギー、キプロス、デンマーク、エストニア、フィンランド、フランス、ドイツ、ギリシャ、ハンガリー、イタリア、ラトビア、リトアニア、ルクセンブルグ、マルタ、オランダ、ポルトガル、ルーマニア、スロバキア、スペイン、スウェーデンにおいては、営業秘密侵害が刑事処罰されうる刑事法の規定が制定された¹⁷⁷。

オーストリア、キプロス、チェコ共和国、デンマーク、フィンランド、ドイツ、ギリシャ、ポーランド、ルーマニアでは、不正競争防止法として、営業秘密侵害が処罰される立法がされている¹⁷⁸。

スウェーデンは、特別法で営業秘密侵害の刑事処罰規定を設けた¹⁷⁹。

このほか、EU 加盟国ではないが、スイスでも、営業秘密侵害が刑事処罰されうるとの規定が同国の不正競争防止法に規定されている。

(2) 親告罪

11 カ国で、親告罪として、処罰されている¹⁸⁰。

(3) 主観的要件

ベルギー、エストニア、フランスでは、過失による営業秘密侵害に、刑事処罰が適用可能とされてきた¹⁸¹。デンマークでは、一定の例外的場合（秘密が広範囲に流布されたなど）には、過失のみで足りるとされている¹⁸²。ハンガリー、イタリア、スウェーデンでは、故意が必要とされているが、目的犯とはされていない¹⁸³。

(4) 関連犯罪

フランスでは、外国権力に秘密情報を提供する行為については、最大 15 年の懲役刑が課される等、厳罰化が規定されている。

より多くの国が、コンピューター犯罪に関して、刑事処罰する規定を置いており、営業秘

¹⁷⁷ 競争会社間での価格設定の合意など、明らかな独占禁止法の違反となる行為は、規制されることが考えられている。欧州委員会、欧州内の営業秘密と機密事業情報の調査（2013）（「欧州委員会調査」）55

<https://ec.europa.eu/docsroom/documents/14838/attachments/1/translations/en/renditions/pdf>

¹⁷⁸ 欧州委員会調査 55

¹⁷⁹ 欧州委員会調査 55

¹⁸⁰ 欧州委員会調査 75

¹⁸¹ 欧州委員会調査 57

¹⁸² 欧州委員会調査 57

¹⁸³ 欧州委員会調査 58

密侵害に関連して、コンピューター犯罪としても取締りが可能となっている¹⁸⁴。

(5) 訴追状況

営業秘密事件が、刑事事件として訴追されることは少ない。その理由として、刑事有罪判決に前提とされる、より高度の確実性（心証）を形成するための立証が難しいこと、合理的な秘密性保持の措置が採られていたことの立証が難しいことがあげられる¹⁸⁵。

(6) 保全的措置

殆どの国で、刑事事件に付随した処分として、証拠保全のための、コンピューターや場所の搜索、差押、被告人の搜索、逮捕、侵害差止命令が、裁判所により発せられることが可能とされている¹⁸⁶。

(7) 刑事罰

① 侵害者個人：大半の国では、懲役刑と罰金とが併科される（15 国）。次いで、懲役刑のみが法定されている国もある（10 国）、6 ヶ月から 3 年の法定刑とされているが、侵害者と営業秘密保有者との関係、侵害者の心理状態、その他の要素で刑が異なることが多い¹⁸⁷。

② 法人罰：従業員や役員の行為について、法人が罰せられることも、オーストリア、ベルギー、キプロス、デンマーク、エストニア、フィンランド、フランス、ハンガリー、ラトビア、ルクセンブルグ、オランダ、ポーランド、ルーマニア、スロベニア、スペイン、英国でみられる¹⁸⁸。

また、スペインや、幾つかの東欧諸国では、法人の解散、事業停止等、厳しい処置が行いいうることとなっている¹⁸⁹。

このほか、スイスにおいても法人罰の規定があり、最高 410 万ユーロまで罰金を課すことができる¹⁹⁰とされている。

(8) 民事救済との関係

多くの国で、民事的な損害賠償の訴えが、刑事事件手続内で扱われているとされる¹⁹⁰。

¹⁸⁴ ベルギー等の加盟国にコンピューター犯罪処罰規定がある。欧州委員会調査 57-61

¹⁸⁵ そのほか、故意や目的といった主観的要素の立証の困難性、多くの国で親告罪であり、民事で和解されると、刑事の進行に影響が出ることも、原因としてある。欧州委員会調査 77

¹⁸⁶ 欧州委員会調査 77

¹⁸⁷ 欧州委員会調査 61-66

¹⁸⁸ 欧州委員会調査 78

¹⁸⁹ 欧州委員会調査 79-81

¹⁹⁰ 欧州委員会調査 76

第4章 営業秘密事件の実務

1 民事的救済措置の付与義務と救済措置の内容（EU 指令第3章第1節）

（1）概要（第6条）¹⁹¹

- ① 加盟国が、違法な営業秘密侵害に対して、民事救済を可能とするために要される、手段、手続き、是正措置を用意しなければならない。
- ② 上記の手段、手続き、是正措置は、以下を充たす。
 - 公正で衡平である
 - 不必要に煩雑、あるいは、高額な、又は、不合理な時間的制約や不当な遅延に服するものでない
 - 効果的で阻止力を有する

（2）比例性と手続濫用（第7条）¹⁹²

- ① 上記の手段、手続き、是正措置は、以下のように実施される必要がある。
 - 比例性を有し
 - 欧州連合内市場での正当な取引へ障害を設けることがない
 - 濫用に対する予防策を用意する
- ② 加盟国は、司法機関が、被告/被申立人の申立てにより、営業秘密侵害が存在するとは到底認められない、又は、申立人が手続きを悪意で利用、若しくは、濫用している場合に、被告/被申立人への損害賠償や、申立人への制裁を含む適当な措置を命ずることができるようにする。上記の措置は、本案とは別の手続きとすることができる。

（3）時効期間（第8条）¹⁹³

- ① 加盟国は、営業秘密侵害に対する手段、手続、是正措置が、実体法上、又は、手続法上、利用可能な期間を一定期間に限定する。
- ② その期間は、6年を超えてはならない。

（4）法的手続中の営業秘密の秘密性の保持（第9条）¹⁹⁴

- ① 関係者による正当な理由ある申立てに応じ、管轄権ある司法機関が、当事者、その訴訟代理人弁護士、若しくは、その他の代表者、裁判所職員、証人、専門家、及び、そ

¹⁹¹ EU 指令第6条

¹⁹² EU 指令第7条

¹⁹³ EU 指令第8条

¹⁹⁴ EU 指令第9条

の他の営業秘密の違法な取得、使用若しくは開示に関連する法的手続に参加している者、又は、これらの法的手続の一部を構成する文書にアクセスできる者が、手続参加、若しくは、アクセスの結果知ることとなった、営業秘密、若しくは、争いのある営業秘密を、秘密であると特定し、使用又は開示することを禁止することを、加盟国は保証しなければならない。加えて、加盟国は、管轄権ある司法機関が、職権で行動することを許すこともできる。

上述の守秘義務は、法的手続きが終了した後も、引き続き有効に存在するが、以下のいずれかの場合に消滅する。

- 最終決定により、営業秘密が、第2条に定められた要件を満たさないことが判明した場合
- 時間の経過とともに、情報が、通常その種の情報を扱う業界内部者の間で、一般的に知られるようになるか、容易にアクセスできるようになった場合。

- ② 加盟国は、管轄権のある司法当局が、当事者による正当な理由ある申立てに基づいて、営業秘密の違法な取得、使用若しくは開示についての法的手続で使用された、あるいは言及された営業秘密、若しくは、争いある営業秘密の、機密性を保持するために必要な特定の措置を、講じることができるようにしなければならない。加えて、加盟国は、管轄権ある司法機関が職権でそのような措置を講じることが許すこともできる。

本項の措置は、少なくとも以下が利用可能とされなければならない。

- 当事者、又は第三者によって提出された、営業秘密、あるいは、争いある営業秘密を含む文書へのアクセスを、全体的若しくは部分的に、限られた数の者に制限すること。
- 営業秘密、若しくは、争いある営業秘密が、開示される可能性がある場合、公開法廷へのアクセスを制限すること、及び、それら訴訟手続に関する記録、あるいは写しへのアクセスを限られた数の者に限定すること。
- 上記限られた数の者に含まれる者以外の者が、営業秘密を含む文章が、削除、又は、編集された、司法判断の非秘密版を利用できるようにすること。

- ③ 前項の措置を決定し、それらの比例性を評価する場合、管轄権のある司法機関は、効果的な救済、並びに、公正な裁判を受ける権利、当事者の、並びに、適切な場合には、第三者の正当な利益、及び、前項の措置の許可、又は、拒否に起因して生じる、いずれかの当事者の、適切な場合は、第三者の、被りうる潜在的危害を考慮するものとする。

2 暫定的措置及び予防的措置（EU 指令第 3 章第 2 節）

（1）暫定的措置及び予防的措置（第 10 条）¹⁹⁵

- ① 加盟国は、管轄権を有する司法機関が、営業秘密保有者の申立てに応じ、侵害者に対し、以下の暫定的、並びに、予防的措置のいずれかを、命じることができることを保証する。
- 営業秘密の暫定的使用又は開示の停止、又は、事情によっては、それらの禁止
 - 侵害品の製造、提供、市場展開、若しくは、使用の禁止、又は、それらの目的のための侵害品の輸入、輸出、若しくは保管の禁止
 - 輸入品を含む、侵害の疑いのある物品の押収、若しくは、送付により、市場への流入、又は、市場内流通の防止
- ② 加盟国は、司法機関が、上記①に代えて、仮想的な営業秘密保有者への損害賠償を充足するに見合う保証金の預託を命じ、営業秘密の使用を許可することができる。

（2）申立要件と保全策（第 11 条）¹⁹⁶

- ① 加盟国は、管轄権ある司法機関が、第 10 条記載の措置に関し、次の事項について、満足できる程度に確実に示すことのできる、提出可能と合理的に見なされる証拠を、提出するよう、申立人に求める権限を有するものとする。
- 営業秘密が存在する
 - 申立人が営業秘密の保有者である
 - 営業秘密が違法に取得されたか、違法に使用、又は、開示されているか、営業秘密の違法な取得、使用、又は、開示が差し迫っている
- ② 加盟国は、管轄権ある司法機関が、申立ての許可、又は、却下の決定で、比例性を検討するに際して、必要に応じ、以下を含む当該事件の特殊な状況を、考慮に入れるようにする。
- 営業秘密の価値、及び、その他の特徴
 - 営業秘密を保護するために講じられた措置
 - 営業秘密を取得、使用、又は、開示する際の、被申立人の行為
 - 営業秘密の違法な使用、又は、開示の影響
 - 当事者の正当な利益、及び、措置の付与又は拒否が、当事者に与える可能性のある影響

¹⁹⁵ EU 指令第 10 条

¹⁹⁶ EU 指令第 11 条

- 第三者の正当な利益
 - 公共の利益
 - 基本的権利の保護
- ③ 加盟国は、管轄権ある司法機関が、下記の場合には、被申立人の申立てにより、措置の取り消し、効力の停止が行われるようにしなければならない。
- 申立人が、措置を命じる司法機関によって決定された合理的な期間内に、又は、20 営業日、若しくは、31 暦日のいずれか長い方を超えない期間内に、事件の実体的審理に至る法的手続を開始しなかった場合
 - 当該情報が、被申立人に帰することができない事由により、第 2 条の営業秘密の要件を満たさなくなった場合。
- ④ 加盟国は、司法機関が、被申立人やその他の第三者に生じうる損失を、補償する保証金の預託を、申立人に命じることができるようにする。

3 本案判断から生じる措置（EU 指令第 3 章第 3 節）

(1) 差止命令及び是正措置（第 12 条）¹⁹⁷

- ① 加盟国は、事件の実体について下された司法的判断が、営業秘密の違法な取得、使用、又は開示があったとした場合、管轄権ある司法機関が、申立人の求めに応じて、1 つ又は複数の、侵害者に対する以下の措置を命じうるものとする¹⁹⁸。
- a. 営業秘密の使用、若しくは、開示の停止、又は、場合によっては、禁止
 - b. 侵害品の製造、提供、市場展開、若しくは、使用の禁止、又は、それらの目的のための侵害品の輸入、輸出、若しくは、保管の禁止
 - c. 侵害品に関する適切な是正措置の採用
 - d. 営業秘密を含む、又は、具体化する文書、物件、材料、物質、若しくは、電子ファイルの全部、あるいは一部の破壊、又は、適切な場合、それらの文書、物件、材料、物質、若しくは、電子ファイルの全部、あるいは一部の、申立人への送付
- ② 上記の c. に記載の是正措置には、以下を含む。
- 市場からの侵害品の回収。
 - 権利を侵害している物品から、権利を侵害している特徴を奪うこと。
 - 権利を侵害している物品の破壊、又は、適切な場合は、市場からの撤退。但

¹⁹⁷ EU 指令第 12 条

¹⁹⁸ 損害賠償と異なり、故意、過失を問わない。第 14 条を参照。

し、その撤退によって、問題の営業秘密の保護が損なわれることはないことを要する。

③ 加盟国は、以下を規定することができる。

市場からの侵害品の撤退を命じるとき、管轄権のある司法機関は、営業秘密の保有者の要求に応じて、その商品を、保有者、又は、慈善団体に送付するように命じることができる。

④ 司法機関は、特段の事情がない限り、上記①c. 及び d. の措置は、侵害者の費用により執行されるよう命じることとする。

(2) 申立要件、保全策、代替措置（第 13 条）¹⁹⁹

① 加盟国は、第 12 条の差止命令及び是正措置の申立てを検討し、それらの比例性を評価する際に、管轄権を有する司法機関が、以下を含む、事件の特殊な事情を考慮に入れることを要求するものとする：

- 営業秘密の価値、又は、その他の特徴
- 営業秘密を保護するために講じられた措置
- 営業秘密を取得、使用、又は、開示する際の、侵害者の行為
- 営業秘密の違法な使用、又は、開示の影響
- 当事者の正当な利益、及び、措置の付与又は拒否が、当事者に与える可能性のある影響
- 第三者の正当な利益
- 公共の利益
- 基本的権利の保護

管轄権を有する司法機関が、上記（第 12 条）第①項 a. 及び b. の措置の期間を制限する場合、侵害者が営業秘密の違法な取得、使用、又は、開示から得た可能性のある、商業的、若しくは、経済的利益を払拭するのに、十分な期間としなければならない。

② 加盟国は、当該情報が、被申立人に直接的又は間接的に帰することができない理由のための第 2 条第① 記載の要件をもはや満たさない場合、被申立人の要求に応じ、上記（第 12 条）第① 項 a. 及び b. の措置が取り消されるか、又は、効力を失うものとする。

③ 加盟国は、第 12 条の措置を命じるにあたり、次の条件が充たされる場合、措置の対象者の申立てにより、金銭的賠償をもって代えうることを規定する。

¹⁹⁹ EU 指令第 13 条

- 使用、又は、開示の時点で、申立人は、その状況下で、営業秘密を違法に使用、又は、開示している他の者から、営業秘密が取得されたことを知らなかったし、知りうべきではなかった。
- 措置の執行が、申立人に不相当な危害をもたらす。
- 原告への金銭的補償により、合理的に、損失を補償することができる。

(3) 金銭的賠償（第 14 条）²⁰⁰

- ① 加盟国は、管轄権のある司法機関が、損失を被った当事者の申立てに応じて、営業秘密の違法な取得、使用、又は、開示に従事していることを知っている、又は知るべきであった侵害者に、営業秘密の違法な取得、使用、又は開示の結果として被った、営業秘密保有者の実際の不利益を補償するのに適切な損害賠償支払いを命じるものとする。加盟国は、故意によらない、雇用主の営業秘密の、違法な取得、使用、又は、開示に対する従業員の損害賠償責任を、制限することができる。
- ② 前項の損害賠償を算定する場合、管轄権のある司法機関は、被侵害者が被った利益の損失、侵害者による不当な利得、経済への悪影響など、すべての適切な要素を考慮に入れるものとし、さらに、営業秘密の違法な取得、使用、又は開示によって、営業秘密の保有者に引き起こされた道徳的偏見など、経済的要因以外の要素も、妥当と判断される限り、考慮されるものとする。
- ③ 司法機関は、適切な場合には、侵害者が、営業秘密を使用するライセンスを求めた場合に支払われるべき、最低限のロイヤルティ、若しくは、手数料額等の要素に基づいて、損害賠償を一括支払額として算定することができる。

(4) 制裁（第 16 条）²⁰¹

EU 指令第 9 条、第 10 条、及び第 12 条の措置に従わない者に対しては、司法機関による制裁を課することができるようにするものとする。また、第 10 条、第 12 条の不遵守に対しては、定期的な違反金の支払を命じることができるものとする。

4 行政措置

(1) 欧州連合

欧州連合では、不正競争に関し、欧州委員会が捜査、訴追する権限を有する。しかし、営業秘密の不正取得、使用を不正競争とした事例は見当たらず、むしろ、営業秘密を他社にシ

²⁰⁰ EU 指令第 14 条

²⁰¹ EU 指令第 16 条

シェアすることを拒否した行為、競争者間での共同での使用を、不正競争防止に関して問題としたことがある²⁰²。技術移転ブロック除外規制²⁰³と 研究開発ブロック除外規制²⁰⁴は、営業秘密の取り扱いについて言及しているが、ライセンスはむしろ競争促進的であると考えられている²⁰⁵。

これに対し、秘密保持契約については、その競争阻害的側面が問題となりうる。もともと、英国、ギリシャ、イタリア、スロベニアでは、規制当局が特に、独占的、又は、寡占的地位にある者が、情報を秘匿し、秘密保持契約に存在する反競争法の問題を規制してきたとされている²⁰⁶。

2018年5月に制定されたヨーロッパの一般データ保護規則（GDPR）は、ヨーロッパ市民に関するデータを扱う企業が、市民のプライバシーに関わるデータを収集、保存、移転する場合に、様々な保護措置等を課すべきことを定めており、情報が収集されている市民に対して、どのような収集がされているかの適切な開示がない場合に、制裁を課することができるものとなっている²⁰⁷。Google に対して、フランスの情報保護当局が、5000万ユーロの罰金を課した事実は有名である²⁰⁸。即ち、情報が個人のプライバシーに関わる場合には、開示が強制されることがあり、営業秘密保護を一定程度制限する。

更に、現在立法化が検討されている The Digital Markets Act（DMA）では、Google などのサーチエンジン、SNS などプラットフォームの運営者に対して、データのシェアを義務づけることで、情報の独占を防止しようとする²⁰⁹。

（2）加盟国当局の規制

ヨーロッパ全体で、営業秘密の不正取得等に関し、不正競争法違反として訴訟が提起され

²⁰² 例えば、Case T-201/04, Microsoft Corp. v. Comm'n, 2004 O.J. (C 179) 36; Case T313/05, Microsoft Corp. v. Comm'n, 2005 O.J. (C 257) 31. Katarzyna A. Czapracka, Antitrust and Trade Secrets: The U.S. and the EU Approach, 24 Santa Clara High Tech J. 207, 209 (2008) 競争会社間での価格設定の合意など、明らかな独占禁止法の違反となる行為は、規制されると考えられている。欧州委員会調査、脚注 177、9-10 頁

<https://ec.europa.eu/docsroom/documents/14838/attachments/1/translations/en/renditions/pdf>

²⁰³ The Transfer of Technology Block Exemption Regulation EC/772/2004

²⁰⁴ The Research and Development Block Exemption Regulation EC/1217/2010

²⁰⁵ 欧州委員会調査、脚注 177、9 頁

²⁰⁶ 欧州委員会調査、脚注 177、50 頁

²⁰⁷ General Data Protection Regulation、規則(EU) 2016/679

²⁰⁸ Adam Satariano, Google Is Fined \$57 Million Under Europe's Data Privacy Law, The N.Y. Times (Jan. 21, 2019) <https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html>.

²⁰⁹ 第 7 章「営業秘密関連の法改正」を参照

ることは稀であり、営業秘密の利用が反競争的とされることも稀とされる²¹⁰。ベルギーでは、競争当局や財務省が職権で、営業秘密事件の捜査を行うことがある。中産階級大臣の要請、公共団体その他の特定の公的機関、若しくは、自然人又は法人の苦情の後、競争に対する危害が発生した場合にも、捜査や訴追がなされることがある²¹¹。ブルガリアでも、競争企業間で営業秘密の不正取得等がなされた場合に、行政的措置が行われる事が可能となっている²¹²。

第5章 域外適用

EU 指令は、欧州連合内の加盟国に対する拘束力を持つ文書であるところ、同指令が対象とする侵害行為、侵害者について、地域的、地理的な制限、あるいは、国籍上の制限は明記されていない²¹³。また、「侵害品」の輸出入が侵害行為に含まれており²¹⁴、営業秘密の不正取得が、裁判地内で起きたことを厳格に必要としないようにも読める。

しかし、EU 指令は、準拠法や管轄権の問題について、明確に扱うことは企図しておらず、欧州連合の既存の法律で決定されることとなることを前提としている²¹⁵。したがって、各加盟国で保護される営業秘密について、準拠法、域外適用についても、各国の判例法、欧州連合の関係する法律により決定される。

第6章 営業秘密侵害の事件数

営業秘密の本案訴訟事件、あるいは、暫定的措置申立事件の処理について、全事件数、処理状況を公開しない加盟国が多く、公開された全事件数として把握することはできない。

なお、欧州連合が行った調査で、営業秘密侵害の被害を受けた（又は、未遂事件があった）と回答した、140 社のうち、わずか 57 社（40.7%）が、裁判所における救済を求めたと回答している。救済を求めなかったと回答した者のうち、その理由としては、証拠収集が困難で

²¹⁰ 欧州連合知的財産権局、営業秘密訴訟のベースライン（2018）（「ベースライン」）、47,48 頁

²¹¹ ベースライン、24 頁

²¹² ベースライン、34,35 頁

²¹³ EU 指令第 1 条

²¹⁴ EU 指令第 4 条

²¹⁵ EU 指令序文第 37 段落「この指令は、司法協力、管轄権、民事及び商事に関する判決の承認と執行のための調和のとれた規則を確立すること、又は、準拠法に対処することを、目的としていない。そのような問題を一般に扱う、他の文書が、原則として、この指令の対象分野に、等しく適用され続けるべきである。」

しかし、違法とはならない情報開示行為等について、「連合法又は国内法にしたがって」と限定が加えられていることなど、地理的な要素が関係する場面は否定できない。EU 指令第 5 条

あったこととした者が最多であった²¹⁶。裁判所において救済を求めた者のうち、以下のとおりに、救済が得られた²¹⁷。

- 証拠の搜索と確保の保全措置(32%)；
- 損害賠償等の金銭的賠償（32%）；
- 侵害者に対する刑事制裁(30%)；
- 侵害行為を禁止する差止命令(28%)；
- 決定の刊行物への公開(15.8%)；
- 侵害品の破壊(10.5%)；
- 税関で侵害品を没収するとの命令(3.5%)；
- 上記のいずれも得られず(17.5%)。

第7章 営業秘密関連の法改正

営業秘密自体ではないが、一部大企業のデータ収集と使用に関係し、個人情報保護のほか、競争を実効化し、消費者を保護しようとする法律の制定が予定されている。欧州委員会は2020年12月、使用・運営の自由を原則としてきたインターネットに、大幅に変化をもたらす、インターネットを利用する消費者、中小企業のアクセスの自由の実質的保障、競争阻害の防止を目的とした2つの法案を提出し、現在も立法化が進んでいる。

1 営業秘密法

EU指令が2016年に策定された後、新たな法制度改正は現在までなされていない。改正の動きは未だない。

2 デジタル化競争政策

2020年以来、The Digital Markets Act (DMA)、The Digital Service Act (DSA)の立法化が進んでいる。²¹⁸DMAは、欧州連合市場内での、インターネット上のプラットフォームの運営と使用に関連しており、市場競争の促進を目的とする²¹⁹。他方、DSAは、プラットフォームに

²¹⁶ 欧州委員会調査、脚注177、143頁

²¹⁷ 欧州委員会調査、脚注177、144頁

²¹⁸ 欧州議会、立法電車スケジュール（DMA経過）（最終アクセス日2022年2月18日）<https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-digital-markets-act>. 欧州議会、立法電車スケジュール（DSA経過）（最終アクセス日2022年2月18日）<https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-digital-services-act>.

²¹⁹ DMA序文

アクセスするユーザーに対して、情報管理システム、実態の透明化、ユーザーの安全確保、誤用や濫用に対する責任の所在の明確化を目的とする²²⁰。

欧州委員会は、3つのオプション（規制対象者や規制内容が固定されたものから、可動性ある、柔軟な仕組みまで）のうち、第2の部分的に柔軟な仕組みを採用することとし、規制対象者は指定されるものの、規制内容については逐次変更ができるようにした。IoTの急速な発展に合致した、柔軟な規制という点で特徴がある。

DMAとDSAは、企業が欧州内に営業所を置かない場合にも、規制対象とするものであり、域外適用とは言えないが、欧州連合内の法益が脅かされるのであれば、対象者に対する管轄権を緩和・拡張して及ぼす点で、GDPRと同様である。

(1) 規制対象者：ゲートキーパー

① 以下で「コアプラットフォームサービス」とは、下記のいずれかを意味する²²¹。

- a. オンライン媒介サービス
- b. オンライン検索エンジン
- c. オンラインソーシャルネットワーキングサービス
- d. ビデオ共有プラットフォームサービス
- e. 番号に依らない対人コミュニケーションサービス
- f. オペレーティングシステム
- g. クラウドコンピューティングサービス

② ゲートキーパーは、以下の条件を充たす、コアプラットフォームを意味する²²²。

- a. 連合内市場に重大な影響を及ぼす（みなし規定があり、少なくとも3つのEU加盟国でのコアプラットフォーム活動²²³があること、及び、例えば、資本時価総額が650億ユーロ以上と考えられる場合、本要件に該当する）。
- b. ビジネスユーザーがエンドユーザーに到達するための、重要なゲートウェイとして機能する、コアプラットフォームサービスを運用する（少なくとも月間4500万人のアクティブなエンドユーザーを有し、年間1万人のアクティブなビジネスユーザーがいる、という閾値をみたすことで、本要件を充たすことが、当初法案で

²²⁰ DSA 序文

²²¹ DMA 第2条(2)

²²² あるいは、欧州委員会の調査により、適用可能であると判断される場合。DMA 経過、脚注 218

²²³ 2021年9月に提出された、欧州議会内、市民の自由、正義、内務に関する委員会意見は、媒介サービスを拡大し、例えば、金融機関でウェブサービスを行う者も含めるべき、とした。DMA 経過、脚注 218

規定されている)。

- c. その運用において、固定した、持続性のある地位を享受する、若しくは、近い将来にそうした地位を享受すると予期される（過去3年間で、上記b.が充たされた場合には、本要件に該当するとされる）。²²⁴

なお、欧州連合議会の主要な政党は、2021年11月17日、市場の売上高が800億ユーロ以上、少なくとも一つのインターネットサービスの提供を行う者を規制対象とすることに合意した（Reuter 報道による）²²⁵。

(2) 規制内容

① ゲートキーパーの義務

第3条(7)に従って特定された、コアプラットフォームサービスのそれぞれに、ゲートキーパーは、以下の義務を負うと規定する²²⁶。

- i. これらのコアプラットフォームサービスから供された個人データを、ゲートキーパーが提供するその他のサービスから得た個人データ、若しくは、第三者のサービスから得た個人データと結合させ、又は、個人データを組み合わせるため、他のゲートキーパーが提供するサービスへ、エンドユーザーをサインインさせることは、エンドユーザーに、特別に当該選択肢を提示し、同意を受けていない限り、やめなければならない。
- ii. ビジネスユーザーが、エンドユーザーに、ゲートキーパーのオンライン媒介サービスを通じて提供される、製品又はサービスを、当該価格とは異なる価格又は条件で、第三者のオンライン媒介サービスを通じて、提供することができるようにしなければならない。
- iii. ビジネスユーザーが、コアプラットフォームを介して取得したエンドユーザーに、サービスオファーを宣伝できること、ビジネスユーザーが、そのためにゲートキーパーのコアプラットフォームサービスを使用するかどうかに関係なく、これらのエンドユーザーとの契約を締結できること、及び、ゲートキーパーのコアプラットフォームサービスを介した、ビジネスユーザーのソフトウェアアプリケーションを使用して、エンドユーザーが、ゲートキーパーのコアプラットフォームを使用しない形で、ビジネスユーザーから取得した、コンテンツ、サブスクリプション、機能、又は、

²²⁴ DMA 序文

²²⁵ Reuter, EU lawmakers agree on rules to target big tech- FT (Nov. 17, 2021)

²²⁶ DMA 第5条

その他のアイテムを、アクセス、若しくは、使用すること、を可能としなければならない。

- iv. ビジネスユーザーが、ゲートキーパーの事業に関連する公的監督機関に、問題を提起することを防止、又は、制限することは、やめなければならない。
- v. ゲートキーパーのコアプラットフォームを介して、ビジネスユーザーが提供するサービスに際して、ゲートキーパーの識別サービスを、使用、提供、相互操作するように、ビジネスユーザーに要求することは、やめなければならない。
- vi. 本条に規定されたゲートキーパーのコアプラットフォームサービスに、アクセス、加入、登録するための条件として、ゲートキーパーのその他の第3条規定のコアプラットフォームサービスに、若しくは、第3条(2)(b)の閾値を充たすものに、参加、登録をすることを、ビジネスユーザー、あるいはエンドユーザーに、要求してはならない。
- vii. 広告サービスを供している広告主、及び、掲載者に対し、その求めに応じて、ゲートキーパーによって提供される、特定の広告の公開、及び、関連する広告サービスのそれぞれについて、掲載者に支払われた金額又は報酬に加え、広告主及び出版社が支払った価格に関する情報を提供しなければならない。

② 特に指定されたゲートキーパーの義務

ゲートキーパーは、第3条(7)規定に従い、コアプラットフォームサービスのそれぞれについて、下記義務を負う²²⁷。

- i. コアプラットフォームサービスのビジネスユーザーの活動を通じて、あるいは、ビジネスユーザーのエンドユーザーの活動を通じて、生成され、利用可能となった非公開のデータ、及び、コアプラットフォームサービスのビジネスユーザーによって提供される、若しくは、これらのビジネスユーザーのエンドユーザーにより提供される、非公開のデータを、ビジネスユーザーと競争して使用することは、やめなければならない。
- ii. 技術的に、第三者によってスタンドアロンベースで提供することのできない、オペレーティングシステム、又は、デバイスの機能に不可欠なソフトウェアアプリケーションに関連し、ゲートキーパーが制限する可能性を損

²²⁷ DMA 第6条

なうことなく、エンドユーザーが、コアプラットフォームサービスにプリインストールされているソフトウェアアプリケーションを、アンインストールできるようにしなければならない。

- iii. 当該ゲートキーパーのオペレーティングシステムを使用、若しくは、相互運用している、第三者のソフトウェアアプリケーション、又は、ソフトウェアアプリケーションストアのインストールと、効果的な使用を、許さなければならない。これらのソフトウェアアプリケーション又はソフトウェアアプリケーションストアが、ゲートキーパーのコアプラットフォームサービス以外の手段で、アクセスされることを許さないとならない。ゲートキーパーが提供するハードウェア、又は、オペレーティングシステムの万全性を危険にさらすことがないように、第三者のソフトウェアアプリケーション、ソフトウェアアプリケーションストアを確実にするための、相당한措置を、ゲートキーパーがとることを妨げてはならない。
- iv. ゲートキーパー自体、又は、同じ事業に属する第三者によって提供されるサービスや製品を、第三者の同様のサービス又は製品と比較し、ランク付けにおいてより有利に扱うべきでない。そのようなランキングには、公正かつ無差別の条件を適用しなければならない。
- v. エンドユーザー向けのインターネットアクセスプロバイダーを含め、ゲートキーパーのオペレーティングシステムを使用してアクセスする、さまざまなソフトウェアアプリケーションとサービスに、エンドユーザーが切り替え、又は、参加する機能を技術的に制限してはならない。
- vi. 利用可能な、又は、ゲートキーパーによる付帯サービスの提供で使用されている、同じオペレーティングシステム、ハードウェア、又は、ソフトウェア機能を、ビジネスユーザーと付帯サービスのプロバイダーが、アクセスをしたり、相互運用性を持つように許さなければならない。
- vii. ゲートキーパーのパフォーマンス測定ツール、及び、広告主と出版社が独自に広告枠を独立して検証するために必要な情報を、広告主とサイト運営者に対し、それらの申請に応じて、無料で提供しなければならない。
- viii. ビジネスユーザー、若しくは、エンドユーザーの活動を通じて生成されたデータの、効果的な移行性を提供しなければならない。継続的、リアルタイムのアクセスの提供を含め、特に、エンドユーザーが、EU 2016/679 規則に準拠して、データ移行性を実行することを、促進するツールを提供しなければならない。

- ix. ビジネスユーザー、並びに、それが提供する製品又はサービスを受けるエンドユーザーによる、関連コアプラットフォームサービス使用のコンテキストで、提供、若しくは、生成される、集約データ又は非集約データを、ビジネスユーザー又はビジネスユーザーが承認する第三者に、効果的、高品質、継続的、かつリアルタイムの、アクセス、ないしは使用を無料で許さなければならない。個人データについては、関連するコアプラットフォームサービスを通じて、関連するビジネスユーザーによって提供される、サービス、若しくは、製品に関して、エンドユーザーによってなされた使用に直接に関連する場合のみ、かつ、エンドユーザーが、規則（EU）2016/679 の意味で、その共有を選択する旨の同意（オプト・イン）したときに限り、アクセス、ないしは使用を許すことができる。
- x. オンライン検索エンジンの第三者プロバイダーに、その申請により、ゲートキーパーのオンライン検索エンジンで、エンドユーザーに生成された、無料検索と有料検索に関連するデータのランキング、検索、クリックと表示に対するアクセスを、公正、合理的、非差別的な条件で、また、個人データを構成する、検索、及び、クリックと表示は、匿名化の上、提供しなければならない。
- xi. 第 3 条に従って指定されたソフトウェアアプリケーションストアへの、ビジネスユーザーのアクセスの、公正で差別のない一般的条件を適用しなければならない。

③ 義務の例外的停止²²⁸

第 32 条（4）の諮問手続に従って、ゲートキーパーは、特定の義務の遵守が、ゲートキーパーの責に帰すことができない、例外的な事情により、ゲートキーパーの欧州連合内事業の経済的存続可能性を危うくすることを理由として、そのような存続可能性の危険に対処するために必要な範囲でのみ、特定の義務の停止を求めることができる。

④ 義務の免除²²⁹

第 32 条（4）の諮問手続に従って、欧州委員会の職権により、又は、ゲートキーパーの申請により、全体的又は部分的に、第 3 条（7）に従い特定された個々のコアプラットフォームサービスに関連して、第 5 条及び第 6 条に規定の義務から免除するこ

²²⁸ DMA 第 8 条

²²⁹ DMA 第 9 条

とができる。

(3) 規制の実施

DMA では第 5 章以下に、事業者が義務に違反している場合に対する規制執行手続が、具体的に記載されている。欧州連合レベルでは、通信ネットワーク、コンテンツ、テクノロジー総指令局が、DMA, DSA の 2 法の所轄官庁となる。新たに創設が提案されている、欧州デジタルサービス委員会 (EBDS) は、独立した諮問グループとして機能し、各国の規制当局を補助するとされる。

第 26 条では、第 25 条に基づく違反決定に際して、年間売上高の 10%を超えない罰金を課せうとしている²³⁰。このような欧州委員会の決定は、CJEU により審査される。

(4) 立法化に対する加盟国の対応、経済社会的影響の予測

ドイツ、フランス、オランダは、DMA が、各加盟国の競争法当局に、より柔軟に規制を行う権限、拡張された規制手段を付与するよう求めている。加盟国の競争法当局は、一致して、競争法当局の権限の拡大を考慮するように声明を出している²³¹。

また、もし DMA が成立すれば、米国に拠点を置く、Google 他の情報通信関連主要 5 社に対して、プラットフォーム上で運営しているユーザーが生成したデータに、ユーザーがアクセスできるようにし、第三者がそのようなプラットフォーム運営者のサービスに相互作用性を持つサービスを提供できるように要求するというものである。現在のところ、そのようなプラットフォームの運営主体である Google、Apple、Amazon、Facebook、Microsoft、Alibaba Group、Bookings.com に適用されるとされる²³²。

3 デジタルサービス適正化

DSA は、近年問題となっている、オンラインでの偽造品、悪意のある表現（ヘイトスピーチ）、偽情報の広がり等、オンラインを利用した違法な取引、違法なコンテンツ配信、その他の危害を及ぼす行為に対して規制し、利用者を保護することを目的とする。即ち、プラットフォームに対し、コンテンツの適正化、プラットフォーム運営の透明化、ユーザーの安全確保、誤用や濫用に対する責任の所在の明確化を求めるもので、2000 年に制定された e-

²³⁰ DMA 第 26 条

²³¹ 欧州議会、立法電車スケジュール (DMA 経過) (最終アクセス日 2022 年 2 月 18 日) <https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-digital-markets-act>.

²³² Reuter, 脚注 225; Makenzie Holland, EU's Digital Markets Act could affect US job growth, TechTarget (Nov. 5, 2021), <https://searchcio.techtarget.com/news/252509188/EUs-Digital-Markets-Act-could-impact-US-job-growth>.

Commerce Directive の改正を伴う。

企業が欧州内に営業所を置かない場合にも規制対象とするものであり、欧州連合内の法益が脅かされるのであれば、対象者に対する管轄権を緩和・拡張して及ぼす²³³。

(1) 規制対象者

オンライン媒介サービスに適用があり、オンラインでの役割、規模、オンラインエコシステムへの影響に応じて、オンライン媒介業者のカテゴリーを設け、異なる義務を課す²³⁴。

- ① ネットワーク基盤プロバイダーによって提供される媒介サービス：コンジットサービス」（例：インターネットアクセス）及び「キャッチサービス」（例：情報の中間的、及び、一時的な自動保存）；
- ② 情報を保存および配布するプロバイダーによって公衆に提供されるホスティングサービス（クラウドやウェブホスティングサービスなどの）
- ③ 売り手と消費者を結びつけるプロバイダーによるオンラインプラットフォームサービス。オンラインマーケットプレイス、アプリストア、共同経済プラットフォーム、ソーシャルメディアプラットフォーム；
- ④ 非常に大規模なオンラインプラットフォーム（又は VLOP）は、月間アクティブユーザー数が 4500 万人を超えるプラットフォームで、特に、経済と社会に特定の影響を与え、違法なコンテンツや社会的危害の流布にリスクを含むため、特定のルールが設定されている。

(2) 規制内容

- ① DSA の範囲内にあるオンライン媒介サービスの、すべてプロバイダーに適用可能な基本的な義務として、サービスの透明性と基本的権利保護する義務が含まれる。これには、そのサービス使用に対し、課す可能性のあるすべての制限を明記する義務が含まれる。
- ② アルゴリズムによる意思決定レビューなど、コンテンツのモデレーションの目的で使用するツールの使用を含む、これらの制限を適用、及び、実施するにあたり、責任を持って行動することが要求される²³⁵。
- ③ 違法なコンテンツと見なされる、又はプロバイダーの利用規約に違反した情報の削除と無効化について報告する必要がある²³⁶。

²³³ DSA 第 1 条

²³⁴ DSA 第 2 条

²³⁵ DSA 第 12 条

²³⁶ DSA 第 13 条

- ④ 最後に、すべての媒介者は、加盟国の当局、及び、その他の管轄当局との直接のコミュニケーションを容易にする単一の連絡先を届け出²³⁷、欧州連合外のもの、は、欧州連合内の法定代理人を指名する²³⁸

(加算義務)	媒介サービス	ホスティングサービス	オンラインプラットフォーム	特大プラットフォーム
透明性報告	●	●	●	●
基本的権利によるサービス条件の制約	●	●	●	●
命令後の加盟国当局との協調	●	●	●	●
連絡先、必要な場合は法定代理人	●	●	●	●
通知と行動、利用者への情報提供義務		●	●	●
訴えと是正、裁判外解決			●	●
信頼された警告			●	●
濫用的通知と対抗的通知への措置			●	●
取引相手の信用調査			●	●
オンライン広告の利用者向け透明性			●	●
犯罪通報			●	●
リスク管理義務と遵守担当役員				●

²³⁷ DSA 第 10 条

²³⁸ DSA 第 11 条

外的リスク監督と公共への説明義務				●
推薦システム透明化と情報アクセスへの利用者選択				●
監督庁や研究者とのデータシェア				●
行動規範				●
緊急事態対応協力				●

(3) 規制の実施

所轄は、国内の規制実施に対して責任を負うデジタルサービスコーディネーター、及び消費者保護委員会（IMCO）となる予定である。DSA の内容とする義務が果たされているかは、当該プロバイダーの主な営業拠点が置かれている加盟国により監督される²³⁹。また、各加盟国は、規制違反に対して、効果的で比例した、抑止的な罰金を用意する²⁴⁰。

(4) サイバーセキュリティ政策

増えつつあるサイバー犯罪による機密情報の漏洩については、特に、米国で規制が強化されているが、欧州連合においても、重点的に安全性を強化する政策が近年拡充してきている。

第8章 国際協力・他国との連携状況

EU 指令は、欧州連合加盟国内で、一貫した保護が営業秘密保有者に付与されることを目的としているので、加盟国内の連携を勧奨し、指令の発効後、定期的に調査報告書が作成されて、欧州委員会に検討されるように予定している。

また、EU 加盟国間の司法、内務関係協力は、欧州連合条約第6編に包含されており、同条約は、「共通の関心事項」に関して協力活動が行われうること、具体的な分野として、民事司法、刑事司法での共助が含まれることを規定する²⁴¹。現在のEUの司法共助・内務協力の活動は、1995年12月に採択されたマドリッド欧州理事会による指針に基づいて行われている

²³⁹ DSA 第40条

²⁴⁰ DSA 第42条

²⁴¹ 欧州連合を設立する条約

EU 加盟国間での捜査共助を調整する機関として知られているユーロポールは、1995 年 7 月に署名されたユーロポール設立条約を根拠に、1998 年 10 月 1 日に正式発足した組織であり、設立後、現在まで機能している。各加盟国は、中央当局からユーロポールを通じて、他の加盟国に対して刑事事件の捜査等へ国際共助を要請することが可能となる。ユーロポールは、EU 他加盟国へ、重大な犯罪への捜査協力の目的で捜査、訴追の協力の要請をする中継機関、情報収集機関となっている²⁴³。中でも、犯罪による収益を追跡し、犯罪物品を没収する機能があるとされ、仮に、国際共助を得られれば、国際的経済犯罪に、捜査、訴追だけでなく、犯罪収益の被害者への還元に有用な手段が得られ、重要な犯罪阻止につながる情報を収集できる可能性がある²⁴⁴。

日本は、EU との間で犯罪捜査に相互に協力するための条約を締結しており、上記のような、欧州内での国際犯罪捜査、訴追の協力のに匹敵した協力要請を行いうる²⁴⁵。例えば、犯罪者の所在地の特定、物件の取得や引渡し等が想定されている²⁴⁶。国際司法共助の中で、最も迅速、効果的に協力が得られることが可能と期待されるのは刑事事件であるものの、欧州加盟国内では、営業秘密の不正な取得等を、刑事事件として捜査、訴追する実務は殆どなく（ドイツで存在するも、非常に少数である）、営業秘密の刑事事件に関する司法共助を、欧州から十分に得られるかには、不明な点が多い²⁴⁷。

この点、EU 指令が制定され、各加盟国で新法が制定、施行されたこと、営業秘密に対する欧州連合内の法的枠組みが相当程度統一され、また、救済が強化されたことは、重要な意味を持つ。最低限の営業秘密保護を与え、侵害に対する民事的な救済措置を整備する結果、欧州連合内に十分な営業秘密の民事的保護のない国が無くなり、欧州連合内の隣接国で侵害行為を行うことで、少なくとも、法の網の目をくぐって営業秘密を不正取得するなどし、民事責任を免れることはできなくなった²⁴⁸。

EU 指令により、著作権、商標権、特許権などの知的財産権に比較しうる保護が受けられる

²⁴² 千田恵介、EU の司法・内務協力の現状（1999）

²⁴³ 千田恵介、EU の司法・内務協力の現状（1999）

²⁴⁴ 千田恵介、EU の司法・内務協力の現状（1999）

²⁴⁵ 刑事に関する共助に関する日本国と欧州連合との間の協定（外務省の HP に情報がまとめられている。https://www.mofa.go.jp/mofaj/gaiko/treaty/shomei_47.html）

²⁴⁶ 刑事に関する共助に関する日本国と欧州連合との間の協定

²⁴⁷ 下記「英国の営業秘密制度」を参照（英国では、営業秘密侵害自体を、刑事処罰する法令がない）

²⁴⁸ 従前より、保護の強い国へ、営業秘密侵害行為により可能となった製品を輸出する行為について、法的権利を行使することは、共犯者とみなされうるような例外的な場合に、一部の国で可能と考えられたものの、非常に困難であった。本書「ドイツ」「英国」編を参照。

ようになった反面、大半の加盟国で、営業秘密は依然として、「知的財産」権には含まれていない²⁴⁹。したがって、営業秘密の保有者が水際で侵害品を摘発し、差し押さえたりなどすることは、EU 法に基づいた形態では不可能である。その結果、営業秘密は、国境において税関職員が侵害品を摘発するといった形で行政的に権利を実現する手段を有しない。但し、水際の救済策は、加盟国の国内法で付与することは不可能ではないので、加盟国ごとに検討がなされる必要がある²⁵⁰。

第9章 仲裁の利用

公開された事件数は見当たらなかったが、営業秘密事件を仲裁手続で解決することは増加していると思料される²⁵¹。

第10章 ライセンス、生産委託、合併会社設立で気をつけるべきポイント

EU 指令により、営業秘密は、「情報を秘密に保つために、合法的に情報を管理している者によって、当該状況下で、合理的な措置が講じられている」と定義され²⁵²、「情報を合法的に管理する者によって、当該状況下で、秘密性を保持するための合理的な措置がとられている」ことが要件となったため、各加盟国法上も、機密情報や営業秘密を、秘密保持義務への合意のないまま、第三者に提供することは、それらの「機密性」を失わせる結果となりかねない²⁵³。具体的な当事者間の事実関係によらず、法律関係を明確化し、将来の紛争を防ぐためにも、秘密保持義務（守秘義務）を明文で盛り込む必要がある。

ライセンスを受けるなどして、機密情報あるいは営業秘密を保持する者が、「秘密性を保持するための合理的な措置」を取っているか否かは、以後の営業秘密の保護に重要な事実として関わってくる。EU 指令では、具体的にどの程度の秘密性保持のための措置が「合理的」とみなされるか、及び、どのような状況下で、問題となった情報が「容易にアクセスできない」情報であるかについて、明らかにされていない。秘密保持義務の内容は、各加盟国の裁判例に応じ、決定される必要があり、そのうち、重要な事項は、秘密保持契約書内に明記さ

²⁴⁹ EU 執行指令（知的財産権の執行指令 2004/48 / EC）、EU 関税執行規則（知的財産権の関税執行に関する規則（EU）No608/2013）

イタリア、ポルトガルは明文で知的財産権に含めており、フィンランドでは、判例上含められ、フランスでは、製法の営業秘密だけを含めている。Intellectual Property Office of European Union, Baseline of Trade Secrets Litigations in EU Member States (2018)

²⁵⁰ Mr. Williams 氏インタビュー

²⁵¹ 英国の営業秘密保護、第9章「仲裁の利用」を参照。

²⁵² EU 指令第2条

²⁵³ 第1章「営業秘密の定義」を参照。

れるべきである²⁵⁴。

(1) ライセンシーにおいて、機密情報、営業秘密を、機密性の程度に応じたラベルをすること、(2) ライセンシー従業員の機密性保持の指導、(3) 情報が、業務を実行するため少なくとも潜在的にアクセスを必要とする人によりのみ開示されている（「知る必要があるベース」）、(4) 情報の開示を受ける者は、秘密保持義務に拘束され、情報に関して、この秘密保持義務を負っていることを認識していることの確認、などが、プラスの要素となるため、ライセンス契約の記載に含めることが推奨される。

ドイツのライセンス契約に含まれる秘密保持契約の参考例は、他の加盟国でもある程度参考となる。ライセンス、生産委託、合併会社設立の際に、当事者間で契約書がかわされる場合、機密保持条項は、通常含まれている。なお、契約の準拠法を決定する場合には、営業秘密保有者の利益が保護されるべき地域と、相手方の事業地域と合わせて検討されることになることと²⁵⁵考えられる。

1 ライセンス契約

(1) 機密情報、営業秘密の特定

ライセンス契約で秘密保持義務を定める場合、機密情報、営業秘密を特定しておくことは重要である。また、EU 指令は、以下の情報を営業秘密から除外している。

- a. 独立した発見や創造
- b. 一般公衆が入手可能であった、若しくは、営業秘密の取得に法的制約を課されていなかった入手者が所持していた、製品や物品の観察、研究、解体、又は、検査
- c. 連合法や法令、慣習に則った、情報及び諮問を得られる、労働者あるいは労働組合の権利の行使
- d. その他、行為時の状況下で、誠実な商慣習に合致した行動

特に、上記 d. に該当する情報が何かが不明確であるところ、契約条項で、適用になる範囲が明確な形で、機密情報、営業秘密が定義され、それが保護されるべきと通常考えられるものであれば、そのような情報を許可なく（権限なく）取得、開示、使用することは「誠実な商慣習に合致」したとは言い難いと考えられる。

したがって、明確で、保護の必要性和バランスのとれた定義とすることが、最終的には、価値ある営業秘密の実効的保護を実現すると言える。また、広範囲すぎる、不明確な条項は、履行が困難であり、現実的でもない。情報の機密性のラベルは、明確化に資し、可能であれ

²⁵⁴ Stuttgart Court of Appeal, Judgement of 19 November 2020 – 2 U 575/19, GRUR-RS 2020, 35613

²⁵⁵ 第 5 章「域外適用」の記述を参照。

ば、採用されるべきと考えられる。

(2) 機密情報、営業秘密へのアクセス、使用目的、使用方法の限定

契約条項を作成する場合、何が許されるか、そして、何が不正取得、使用、又は、開示になるかを明確にすることは、ライセンシー及びライセンサーの利益を守り、また、有効な関係を維持するためにも大切である。例えば、ライセンシー側で、パスワード等アクセス制限を設定すること、アクセスできる者を、一定の被用者、関係会社の被用者、専門家、監査人等に制限すること、アクセスの目的と使用方法を制限することなどが考えられる。

侵害行為者が、営業秘密の不正使用、開示、取得にあたる事実を認識していたことや、認識すべきであったことが、営業秘密侵害の前提とされており、許可事項と不許可事項を分別することが意味を持つと考えられる。

(3) 契約終了後の情報の返却あるいはデータ削除義務

秘密保持義務の内容として、提供された機密情報、営業秘密は、契約関係終了時に保有者に返却すること、また、バックアップも含めて、保存されたデータから削除するように要求すること、それを確認することの2点を明記することが必要である。これは前記の、機密性を保つ合理的な措置の認定にも、プラスの要素として働くと考えられる。

(4) 補償条項

相手方の秘密保持義務違反の結果生じた損害について、相手方に補償の義務を負わせることは、契約に含められることが少なくない。

(5) 損害額

機密情報・営業秘密保有者は、不正取得、使用、あるいは、開示により生じた損害に対する賠償として、特約がない場合、自分の被った損害を立証して、その填補を求めることができる。この損害の立証は、裁判上困難となることも考えられるので、損害額の算定について、事前に合意しておくことも考えられる。

(6) 仲裁合意

裁判による紛争解決と比較し、仲裁は、営業秘密、機密情報の保護に適していると一般に考えられている。この理由として、営業秘密保有者が主張した内容、提出あるいは開示した情報の秘密性が保たれることが、通常あげられる。そこで、ライセンス契約にあたっても、仲裁条項を挿入して、仲裁により契約の紛争を解決し、ライセンサーとライセンシーの双方の機密情報や営業秘密の保護を図ることは、積極的に検討されるべきである。

2 生産委託契約

上記に列挙した注意点は、生産委託契約にも当てはまる。

委託者としては、受託者の生産ラインの運営状況、生産品の数量等確認体制、保存・管理状況を十分確認することが、特に重要となると考えられる。そこで、契約書にも、これらの事項について、受託者に報告、保証、あるいは誓約をするよう義務づけることは検討されるべきである。

生産委託契約では、受託者が、第三者の機密情報、営業秘密情報をたまたま持っていて、委託者の製品の製造に使用してしまった場合、第三者から、機密情報・営業秘密の不正使用、開示にあたるとして請求をおこされてしまう可能性がある。委託者自身が知り得ない場合、受託者に対して差止命令などが発せられたり、発令された措置により生産に対する影響が起こりうる。そこで、生産された製品が、受託者と取引関係のある、他社の機密情報・営業秘密の侵害をしないことを誓約する、保証を要求することは検討されるべきである。

機密情報、営業秘密へのアクセス、使用目的、使用方法の限定に関して受託者から第三者への再委託を禁止することも考慮すべきである。

3 合弁契約

合弁会社は、参加当事者が提供した、あるいは、合弁会社自身が調達した人材、技術、データ、施設、及び、資材を使用して、事業を行うことが多い。参加者の様々な機密情報、営業秘密が提供されることもある。

したがって、合弁会社が研究や開発をして得られる成果物に対して、どの者に所有権あるいは管理権が帰属するのかを契約で明確化しておくことは特に重要となる。

ドイツ

第1章 営業秘密の定義

ドイツはEU加盟国であるため、EUの指令や規制に従って国内法の整備・改正がなされる。ドイツにおける営業秘密の保護に関する法律は、2016年6月9日EU指令²⁵⁶の国内実施のために制定され、2019年4月18日に発効した²⁵⁷。2019年まで、ドイツではさまざまな法律や規制が、営業秘密の保護に適用されてきた。この中には、ドイツ不正競争法（UWG）、ドイツ刑法、ドイツ財政法、ドイツ民法（BGB）、ドイツ株式会社法、ドイツ競争制限法（ARC）が含まれる。1896年から2019年まで、主に営業秘密保護に適用された法律は不正競争法（UWG）²⁵⁸で、UWGに関する刑事事件や民事事件の判決によって、営業秘密の保護がなされてきた²⁵⁹。したがって、新法 GeschGehG に営業秘密の定義規定を置き、規制・救済の対象となる不正な営業秘密の取得、使用、開示行為を明確化した²⁶⁰。新法が UWG を置き換えたこととなる。

そこで、本報告書では、ドイツ法における営業秘密の定義について、かつての UWG（第17条～第19条）に関する判例法で示された考え方と、EU指令を受けて2019年に発効した営業秘密の保護に関する法律（GeschGehG）が規定している定義内容について紹介する。

1 判例法による定義

従前の UWG の第17条～第19条に関して発展した判例法では、下記の要件を満たすものについて営業秘密としての保護を認めていた。

- a. 非公知で、容易に入手できない、限られた数の者にのみ知られており、

²⁵⁶ EU Directive 2016/943 (Directive)

²⁵⁷ Gesetz zum Schutz von Geschäftsgeheimnissen(略称「GeschGehG」)

²⁵⁸ Gesetz gegen den unlauteren Wettbewerb : UWG 第17条から第19条

²⁵⁹ ドイツの不正競争法（UWG）には、特定の不正流用行為に対する営業秘密の保護に焦点を当てた、第17条、第18条、第19条が規定されていた。従業員による営業秘密の第三者への違法な開示を禁止しているだけでなく、第19条は共犯者の行為を処罰し、更に、産業スパイ、つまり、従業員、若しくは、第三者による技術的手段の適用による、営業秘密の不正使用も禁止されていた。新法がこれらの規定を置き換えることとなる。Thomas Nagele, et al., Trade Secrets 2021, Chambers And Partners (Apr. 28, 2021), <https://practiceguides.chambers.com/practice-guides/trade-secrets-2021/germany/trends-and-developments>

²⁶⁰ GeschGehG 第4条。経済産業省「諸外国における営業秘密保護制度に関する調査研究報告書」（2014）、特許庁「人材の移動による技術流出に係る知的財産の在り方に関する調査研究報告書」（2011）、経済産業省「諸外国の訴訟手続きにおける営業秘密保護の在り方等に関する調査研究報告」（2010）がある。

- b. 特定の事業にかかわる、
- c. 技術的又は非技術的情報で、
- d. 情報を保有する者の意図によって秘密とされている²⁶¹。

このように、営業秘密の存在に関して客観的な事実から認定できる秘密性の存在を明確に要求してこなかった²⁶²。このため、営業秘密保有者が主観的に秘密であると判断し、実際に商業的価値がある情報については、営業秘密保有者がどのようにして秘密性を保持していたかが詳細に審理されることはなかった²⁶³。

2 GeschGehG による定義²⁶⁴

GeschGehG 第 2 条は、EU 指令の内容を取り込んだものとなっており、何が営業秘密となるかについて、以下のとおり定義している。

- a. 集合体として、又は、その正確な構成や要素の組立てに関して、当該情報と同種の情報を通常扱う業界の内部者で、一般に知られておらず、又は、容易にアクセスすることができない点において、秘密にされている。
- b. 情報を合法的に管理する者によって、当該状況下で、秘密性を保持するための合理的な措置がとられている。
- c. 秘密性を保持することについて、正当な利益が存在すること

GeschGehG の定義では、秘密性確保のための合理的な措置が採られていたことを要件としている。また、「秘密性保持に関する、正当な利益の存在」が必要となる。「正当な」という限定が付されていることからして、営業秘密保有者自身の私的な利益を超えて、公的に見ても、保護に値する情報であるかが問われる可能性がある。この点について英国 TS 規則で採用された定義と比較すると、商業的価値の有無を格別に問題としていない点で異なる²⁶⁵。

(1) 秘密性保護の措置

従前、営業秘密の存在を認めるために、裁判所は、最適の保護措置がとられている必要はなく、個別の事件の事実関係に即して、相当性の観点から判断する、とのみ述べていた²⁶⁶。

一方で、裁判所の中には、個々の営業秘密に対する保護措置が採られている必要があると述

²⁶¹ 連邦裁判所は、営業秘密の存在に関して、事実の発見が、秘密の所有者に経済的損害を引き起こす可能性があるため、所有者が、秘密性確保に正当な利益を持っていることを要求した。

Maria von Tippelskirch 氏インタビュー

²⁶² 前掲 Nagele, et al.

²⁶³ 前掲 Nagele, et al.

²⁶⁴ GeschGehG 第 2 条

²⁶⁵ 営業秘密規則第 2 条

²⁶⁶ Dusseldorf Regional Labor Court, Judgment of 3 June 2020 – 12 SaGa 4/20

べたものもあり、混乱が生じていた。

このような中、シュトゥットガルト控訴裁判所は²⁶⁷、「情報を秘密に保つための合理的な措置」の最低基準に関する判例を確立しようとした。同裁判所は、下記を考慮することを判示した。

- a. 営業秘密の性質と価値
- b. 当該事業にとっての営業秘密の重要性
- c. 研究と開発に要した費用
- d. 事業の規模
- e. 事業において通常にとられている安全策
- f. 情報のラベルの仕方
- g. 従業員や取引先との契約中での言明

また、同裁判所は、次のような事実の有無を重要視することを明らかとした。

- i. 情報は、割り当てられた仕事を実行するため、少なくとも潜在的にアクセスを必要とする人にのみ開示されている（「知る必要があるベース」）、
- ii. 情報が開示される人は、秘密保持義務に拘束され、情報に関して、この秘密保持義務を負っていることを認識している。

その上で、同裁判所は、所有者に秘密保護の不備がある場合は、所有者が追加の保護措置をとったかどうかに関係なく、適切なレベルの秘密の保護がない状況と認定される結果につながる可能性があると判断した。特に、従業員が、パスワードによる保護なしで、自分のハードウェアにファイルを保存することを容認することで、「データ漏洩」の危険にさらす、または、紙の文書が関係している場合は、無許可の者が、紙の文書を閲覧しうる状態にあったなど、保護に不備があることによって、通常、秘密の適切なレベルの保護を否定する場合がある。

(2) 新法と旧法の差異

以上のとおり、新法の定義では、秘密性を保つための合理的な措置がとられていることを明確に要件としていることから、旧法において営業秘密とされていた情報が、営業秘密にあたらなくなる可能性はある。

この点に関連して、シュトゥットガルト控訴裁判所の示した要件は重要と考えられ、営業秘密を知る必要がある関係者間のみでシェアされていたか、秘密保持義務が課せられていたか、パスワード管理がされていたか、記載された有体物の管理が厳格にされていたか、は営

²⁶⁷ Stuttgart Court of Appeal, Judgement of 19 November 2020 – 2 U 575/19, GRUR-RS 2020, 35613

業秘密該当性を判断する上で、検討されることになると思われる。

第2章 営業秘密侵害行為の定義

1 従前の判例法における営業秘密侵害行為

UWG 第 17 条から第 19 条では、侵害行為となるのは、基本的には、従業員が、故意又は過失により、営業秘密を不正に開示、取得又は使用した場合であり、従業員以外の者については、教唆等の積極的な意図・意欲（単に、営業秘密であるという認識、故意だけでなく）が伴っていることを要求していた²⁶⁸。

2 新法における営業秘密侵害行為

(1) GeschGehG 第 4 条によると、次の行為を営業秘密の侵害行為と規定している。

- a. 営業秘密の保有者の合法的な管理下にあり、営業秘密を含む、又は、営業秘密を取り出さうな文書、物件、材料、物質、又は、電子ファイルへの許可を得ないアクセス、使用、若しくは、コピー、又は、当該状況下において、誠実な商慣行を考慮して、信義誠実の原則に反するその他の行為。
- b. 次に該当する者による、営業秘密の使用または開示する行為。
 - i. 前項の規定により営業秘密を自ら取得した者
 - ii. 営業秘密の使用制限義務に違反している者
 - iii. 営業秘密を開示しない義務に違反している者
- c. 他人を通じて営業秘密を取得し、その取得、使用又は開示の時点で、他人が前項に反して、営業秘密を使用又は開示していた事実を、認識していたか、若しくはその行為時の状況下で、認識すべきであった場合。これは、使用が、これらの目的のための、侵害品の生産、提供、市場展開、輸入、輸出、又は、保管からなる場合に、特に適用される。

(2) 第三者の行為

GeschGehG 第 4 条により、侵害行為は、広げられた概念で決められるようになり、従業員以外の者について、積極的な意図・意欲のみならず、過失により営業秘密の不正な開示、取得、使用をした場合においても、民事的救済を受けることが可能となった²⁶⁹。このため、例

²⁶⁸ 前掲 Nagele, et al.

²⁶⁹ 第 4 条は、取得、開示、または、使用する時点で、その状況下で、営業秘密が、違法に開示あるいは使用していた者から、直接または間接に取得された事実を知っていたか、知るべきであった場合には、営業秘密の侵害とする。なお、EU 指令では、当初は営業秘密であることを知らず、後に不正に開示された営業秘密であったことを認識した場合も、侵害行為とし

例えば、不正に取得された営業秘密を使用している製品やサービスを、作出、販売、輸出入、市場に提供する者の行為を対象として、民事的救済措置（金銭的損害賠償を含む）を求めることができるようになった²⁷⁰。

(3) 侵害における主観的要件

EU 指令の第 14 条（1）によると、加盟国は、被用者が、雇用主の営業秘密を、違法に取得、使用、または開示した場合に、故意を欠くときには、その法的責任を緩和することができることとなっている。この点に関して、ドイツではこのオプションは適用されていない²⁷¹。他方で、営業秘密の侵害に基づく金銭的損害賠償は、GeschGehG の第 10 条（1）に従って、侵害者が少なくとも過失で行動したことが必要となる。ただし、これまでのところ、この GeschGehG の第 10 条に関連する公開された裁判所の決定は見あたらない。

(4) 除外規定

GeschGehG 第 5 条は、どのような営業秘密の取得、使用又は開示行為が例外的に許されるか規定している。内部告発のための情報の開示など、公共の利益を目的とした行為を、侵害行為から除外している²⁷²。

- a. メディアの報道の自由、多様性を含む、表現、及び、情報の自由の権利行使。
- b. 取得、使用、又は、開示が、違法行為、不正、その他の不法行為を明らかにするのに役立つなど、一般の公益を保護するのに適している場合（内部告発者システムの組織において、法第 5 条第 2 項の規定に加えて、まもなく発効する連合法違反を報告する者の保護に関する指令（EU 2018/0106）の規定）を考慮に入れる必要がある。
- c. 従業員代表が、その職務を遂行できるようにするために必要な場合、従業員が、従業員代表へ、秘密とされる情報の開示をする場合（法第 5 条第 3 項）。これには、例えば、従業員の代表が差し迫った人員削減について通知した場合など、合法的なグループの利益の追求が含まれる可能性がある。

3 新法と判例法の差異

新法により、営業秘密侵害行為の範囲は、営業秘密保有者と直接の取引関係がない第三者（いわゆる転得者）の行為にまで及ぶようになった。したがって、営業秘密侵害の故意が通常無いような転得者が、侵害品を製造したり、販売したり、輸入した場合であっても、侵害

てカバーする。ドイツにおいては、行為者のとった行為（開示や使用）の時点での心理的内容を問題としている。

²⁷⁰ 前掲 Nagele, et al.

²⁷¹ 第 11 条

²⁷² 同法第 5 条

している事実について、知るべきであった（過失があった）と立証できる限り、そのような第三者に対して民事的救済を請求することもできるようになった。

第3章 営業秘密侵害に関連する法律、規制の概要

1 GeschGehG

(1) 証拠収集／保全措置²⁷³

営業秘密保有者は、侵害者に対して、次の情報を請求する権利がある。

- a. 侵害製品の生産者、供給者、並びに、他の以前の所有者、及び、意図された顧客と販売店の名前と住所
- b. 製造、注文、配送、又は、受領した侵害品の数量と購入価格
- c. 営業秘密を含む、若しくは、具体化する、侵害者が所有、又は、保有する文書、物件、材料、物質、または電子ファイル
- d. 営業秘密を入手したであろう者、営業秘密を開示した相手

(2) 救済

GeschGehG は、営業秘密保有者は、侵害者に対して、次の救済を受ける権利がある可能性があることを明確にしている。

- 侵害排除措置（第6条）
- 侵害品の破壊、リコールなどの特別措置（第7条）及び
- 会計情報と補償（第8条）

つまり、第6条で、営業秘密保持者の申立てに応じて、裁判所は、暫定的措置として、営業秘密の使用、若しくは、開示の禁止、並びに、停止、及び、文書、物件、材料、物質、又は、電子ファイルの差押えを命じることができる。

また、第7条の規定により、本案（主な手続き）に関して下される裁判所の決定では、以下を命じることができる。

- a. 営業秘密を含む、若しくは、具体化する、侵害者が所持、若しくは、所有する文書、物件、材料、物質、又は電子ファイルの破壊または没収
- b. 侵害品のリコール
- c. 流通経路からの侵害製品の永久的な除去
- d. 権利を侵害している製品の破壊
- e. 営業秘密の保護に影響がない場合は、侵害品の市場からの撤退
- f. 損害賠償²⁷⁴

²⁷³ 同法第8条

²⁷⁴ (1) 第11条は、故意、若しくは、過失のいずれもみたさない侵害者が、侵害者が、請求の履行により過剰な不利益を被る場合、かつ、金銭による補償が適切であると思われる場合、第6

(3) 訴訟手続

恒久的措置や暫定的措置の発令にあたり、裁判所は、裁量により、口頭での審理なし、完全に対審なし、又は、口頭審理後に決定する、のいずれかを選ぶことができる。原則として、差止命令と差押えとが双方同時に申し立てられた場合、口頭審理も、侵害者の審尋も開かれなない。そうしないと、警告によって、侵害の事実を隠匿するリスクがあるためである。そのような事情が確実に証明され、権利が明確である場合、事前に被告の意見を聞く理由はないとされる。

(4) 時効

民事上の請求権については、3年間の通常の時効の対象となる²⁷⁵。ただし、特別規定として、第13条では、侵害者が、特別な状況下では、損害賠償請求権の時効による消滅後であっても、取得した商品を放棄する義務があることを規定している。これは、6年の除斥期間に服する。

(5) 刑事罰

競争上の利益を図るため、自己の利益のため、第三者の利益のため、または、営業秘密保有者に損害を与える目的で、(i)不正使用、開示、取得した者、もしくは、(ii)他人を通じて取得した営業秘密を使用、開示した者には、最高3年の懲役または罰金が科せられ、競争上の利益を図るため、または、自己の利益のために、取引の過程で業務上委託された技術的性質の秘密文書または規則である営業秘密を使用、開示した者は、最高2年の懲役または罰金が科せられる²⁷⁶。

産業スパイ、営業秘密の海外利用事案については、最高5年の懲役または罰金が科せられる²⁷⁷。

条または第7条に基づく請求を回避するために、営業秘密の所有者に金銭賠償することができると規定する。

(2) 賠償金額は、ライセンスを契約上付与する場合に、適切と考えられる額に基づく。営業秘密の保有者は、差止命令を受けられる期間以上の期間に対して、補償を求めることができない。

(3) 損害定量化は、3つの方法から選択できるとされている。実際に発生した損害の賠償を要求するか、侵害者が行った利益の返還を要求するか、または、営業秘密を取得、使用、または開示することに同意を得た場合に侵害者が支払わなければならなかったであろう適切なロイヤリティに基づいて損害を計算することができる。

²⁷⁵ BGB 第195条、第199条

²⁷⁶ GeschGehG 第23条第1項から第3項

²⁷⁷ 同条第4項

未遂犯も罰せられる²⁷⁸。

訴追にあたっては、原則として、被害者の申告が必要とされる²⁷⁹。

2 刑法

ドイツ刑法は、営業秘密の取得、使用、あるいは、開示行為を、犯罪として処罰する²⁸⁰。

- a. 第 203 条は、専門家（医師、歯科医、心理学者、弁護士又は弁理士）としての立場で、他人の事業秘密または営業秘密を不法に開示した者に対して、最高 1 年の懲役または罰金を科す。
- b. 第 204 条は、第 203 条に従って秘密を保持する義務がある者が、他人の秘密、特に、事業秘密または営業秘密を違法に使用した場合の、2 年以下の懲役または罰金の賦課を規定する。第 202a 条（データスパイ）は、不正アクセスから保護されており、直接に他人に認識されえない、又は、送信されない方法で保存されたデータを許可なく取得する行為を犯罪とする。これには、秘密の取引データ、及び、事業データが含まれる。罰則は、最高 3 年の懲役又は罰金とされている。
- c. 第 355 条（1）2 は、公務員が、営業秘密、事業秘密を違法に開示、又は、使用した場合に対する罰則として、2 年以下の懲役または罰金を定める。
- d. ドイツでは、刑事責任は法人には適用されない。
- e. 未遂犯は罰せられない。

3 民法

- (1) 従業員は、BGB 第 242 条の一般的な誠実な履行条項に従って、雇用主の営業秘密、及び、事業秘密を秘密に保つ義務がある。従業員は慣習を考慮し、信義誠実の原則に従って履行する義務がある。

雇用中、守秘義務違反が発生した場合、雇用主は通知なしに従業員を解雇し、損害賠償を請求することができる。

しかし、雇用主の特別な利益によって正当化されない、従業員に対する過度の義務を課す条項は無効とされる。

従業員は、雇用後も営業秘密に対する守秘義務を負うが、仕事から得られたスキルや知識は、守秘義務に含まれない。

- (2) 取引関係を意図して交渉を行う企業は、営業秘密を含む可能性のある機密情報を互いに

²⁷⁸ 同条第 5 項

²⁷⁹ 同条第 8 項

²⁸⁰ ドイツ刑法は、第 203 条、第 204 条、第 202（a）条、および第 355 条（1）に基づいて営業秘密の保護を規定しており、それぞれ、個人秘密の侵害、他者の秘密の悪用、データスパイ、および税務秘密の違反を処罰する。

共有することがよくある。BGB は、第 311 条及び第 241 (2) 条に基づいて、相手方の権利および法的利益を保護しなければならないと規定している。

4 商法

ドイツ商法第 164 条により、機密保持条項と競業避止条項は、元従業員が合意された競業避止義務に対して、一定の報酬を受け取った場合にのみ有効であるとする。また、競業避止条項についての法定の上限期間（制限）は 2 年である。

5 その他関連法改正

(1) 特許法

GeschGehG の制定に伴い、ドイツ国内で、営業秘密保護強化に付随する制定法の改正作業がみられている。例えば、ドイツの特許法（「Patentgesetz」、略称：「PatG」）は、2021 年 8 月 18 日に改正された。この改正では、営業秘密や機密情報保護の強化を受けたもので、PatG への新しい第 145a 条の追加が含まれる。この PatG の第 145a 条に従い、GeschGehG の第 16 条から第 20 条が特許訴訟に適用されるようになったことが重要である。つまり、GeschGehG の第 16 条から第 20 条は、裁判所が「訴訟の対象となる情報」の機密扱いを義務付けているので、今後の特許侵害訴訟においては、当事者の機密情報や営業秘密が、不必要に開示あるいは不正に使用されないように対策が講じられる。ただし、この「訴訟の対象となる情報」という概念について、学術文献ではかなり曖昧であると指摘されている²⁸¹。

上記に関連して、PatG の第 145a 条は、「訴訟の対象となる情報」という用語を「原告または被告によって係属中の訴訟に投入された情報」と定義しており、おそらく、PatG の第 145a 条の定義は、GeschGehG の第 16 条の同じ用語の解釈に直接影響を与えないと解されるが、PatG の第 145a 条の定義が、少なくとも判例法によって、最終的に GeschGehG 第 16 条に導入されると考えられるところである。

(2) 実用新案法

前掲(1)で紹介した特許法と同じことが、ドイツの実用新案法

（「Gebrauchsmustergesetz」、略称：「GebrMG」）の新しい第 26a 条にも当てはまる。同条は第 145a 条 PatG と同様の規定を置くものであり、2021 年 8 月 18 日に発効した。

²⁸¹ Alexander in : Köhler/ Bornkamm / Federsen、UWG、第 39 版 2021、及び、GeschGehG 第 16 条欄外 25 を参照

第4章 営業秘密事件の実務

1 知的財産権訴訟の訴訟提起および証拠収集段階における営業秘密の保護

ドイツの民事訴訟法は、米国のように、ディスカバリーを特徴・制度の一つとして有していない。それでも、営業秘密の保有者が営業秘密侵害を主張したい場合に、秘密を開示等してしまう危険は内在する。

初めに、EU 指令に基づき、営業秘密は、実際に秘密である場合に限られる。つまり、関連する業界内で広く知られていない場合、ドイツ法下で保護される。この点、すべての情報が保護されるわけではない（一定範囲でしか保護されない）ことを理解しなければならない。次に、営業秘密の違法な使用、取得等を実証するには、営業秘密の具体的な記載が必要であることも重要である。したがって、所有者が、必要に応じて、営業秘密を「開示する」必要がある。それによって、営業秘密が、相手方に知られる危険にさらされる。このリスクを軽減することが、上記の GeschGehG の第 16 条から第 20 条の主な目的である。

営業秘密訴訟において営業秘密を保護するメカニズムは、GeschGehG の第 16 条から第 20 条に含まれている。その詳細は、次のとおりである。当事者による申請により、裁判所は、特定の情報が機密情報であることを確定できる。この場合、訴訟に関与する者、例えば、当事者、その代理人、証人、専門家が、訴訟の目的を超えて、訴訟手続において提示された機密情報を使用、または、開示することが禁止される。また、第三者のファイルにアクセスする場合、機密情報は記録から省略される。

(1) Dusseldorf Court of Appeal, Judgment of 11 January 2021 - 20 W 68/20, GRUR-RS 2021, 7875 ff

この決定は、ドイツの著作権法第 87a 条以降の規定に基づく、データベースの保護に係るものである。原告は、問題となっているデータベースについて、アクセスを被告に提供すべきものではないことを理由として、データベースの内容について、決定することを拒否した。その代わり、原告は、GeschGehG の第 16 条に基づく措置を申請した。

デュッセルドルフ控訴裁判所は、GeschGehG 第 16 条以降は、営業秘密に関係のない手続に適用はされないと判断した。デュッセルドルフ控訴裁判所は、GeschGehG 制定の公式資料から、機密保持に関する規則は、営業秘密に関する（BT-Drs. 19/ 4724, 34 を参照）訴訟にのみ適用される、という立法者の声明を確認し、同判断に至る理由とした。このような GeschGehG 第 16 条以降の制限的な適用は、同法制定以来、ドイツの法律学者によって批判

されていたところである²⁸²。

なお、本論点に関しては、2020年10月28日のカールスルーエ控訴裁判所の判決でも、結論が下されないままとなっていた²⁸³。

本決定で、デュッセルドルフ裁判所が同条の適用範囲を制限したことが、新しく PatG の第 145a 条、および、26aGebrMG が制定されることとなった理由である²⁸⁴。

- (2) Stuttgart Court of Appeal, Judgment of 19 November 2020 - 2 U 575/19, GRUR-RS2020, 35613

実質的に、また、機能的にも、GeschGehG は、UWG の第 17 条から第 19 条を書き換える。UWG の第 17 条は、GeschGehG が発効した日に廃止された。しかし、GeschGehG には移行規定は含まれていない。したがって、営業秘密侵害時に該当する UWG 第 17 条が法的に有効であった場合、営業秘密保有者が、そうした過去の侵害に基づいて、侵害者に対して営業秘密訴訟を開始し、GeschGehG を遡及的に適用することも考えられる。これが、シュトゥットガルト控訴裁判所が判断をした事件において問題となった。裁判所は、当事者による最初の行動が、GeschGehG ではなく、UWG 第 17 条によって規律されていたとしても、当事者が GeschGehG の規定に基づいて申し立てれば、第 16 条以降の守秘義務を課す措置を適用することは可能とした。

- (3) Hamm Court of Appeal, Judgment of 27 January 2021 - 20 W 48/20, BeckRS 2021, 14668

ハム控訴裁判所は、通常、営業秘密と見なすことができる情報が、訴訟中に守秘義務の命令なく、提出物として裁判所に提出されることで、一般に知られるようになるとは限らず、営業秘密としてのステータスと保護を、必ずしもそれで失うことにはつながらないと述べた。それは、裁判所の訴訟手続中に提出物へのアクセスが許可されるのは、通常限られた何人かのグループの者であり、情報が一般に知られるようになることにつながらないと考えたためである。更に、裁判所は、複数の訴訟手続きの提出物として情報を提出することさえ、守秘義務を課さなくても、情報を一般に知らしめることにつながらないとした。

2 救済手段、営業秘密保護の現状

ドイツ民法下では、不法行為の被害者に認められる救済手段として、従来、金銭的賠償、不

²⁸² GeschGehG (Hauck in : GRUR-Prax 2019, 223, 225, Semrau-Brandt in : GRURPrax 2019, 127, 128; Schregle in : GRUR 209, 912, 913 を参照)

²⁸³ 6 W 35/20, BeckRS 2020, 90799

²⁸⁴ 上記第 3 章 5「その他関連法改正」を参照

当利得返還、侵害製品の破壊が認められてきた²⁸⁵。営業秘密保有者は、差止めによる救済、金銭的賠償、保護された情報の返却又は破棄、損害賠償を計算する基礎とする利益に関する情報の提供、搜索命令、特定の文書提出命令、暫定的措置等の救済を利用できる。

ただし、裁判所が救済を与えるにあたり、他の法益とのバランスが重要とされており、被用者に対して、労働の自由を不必要に制限することとなる場合には、秘密保持義務はその効力を否定されてしまうことがある。また、雇用期間終了後に、被用者に課される制約（例えば、取引先を自らの顧客として勧誘したり、他の従業員を従業員等として勧誘したりすることの禁止）は、従前の3年間の平均給与のおよそ50%の支払をする場合にのみ有効であるとされている²⁸⁶。

これらの救済措置は、GeschGehGの発効後、GeschGehGで許可されている上記救済策と並行して、引き続き有効に存続し、利用することが可能である。

(1) 本案判決による作為又は不作為義務を課す命令

① 排除措置命令および差止命令

ドイツの法律では、権利がすでにあることについて争いがない場合、権利侵害された時点で、繰り返しのリスクがあるため、被告が、すでに権利を侵害しているかどうかによって、侵害の危険性の認定に差異が生じる。被告は、契約上のペナルティによってサポートされる、侵害の中止と中止の宣言によってのみ、排除措置命令や差止命令を回避できる。また、過去に被告の侵害がなかったが、初めて侵害の危険性が生じている場合には、侵害に該当する行為はしないという、被告の拘束力のない宣言によって、命令を回避することができる。

シュトゥットガルト控訴裁判所は、営業秘密の侵害は単一の現象ではないが、3つの個別のタイプの侵害（違法な取得、使用、開示）は個別に扱われなければならないと認定した²⁸⁷。その結果、違法な営業秘密の取得は、違法な取得に関して繰り返されるリスクを生み出すだけとされた。そこで、違法に取得した営業秘密の使用・開示については、最初の侵害の危険性が生じているのみであり、不法に取得した侵害者が、侵害行為をしない旨の拘束力のない宣言を行うことにより、取得した営業秘密の使用と開示に関する差止命令を免れることができる²⁸⁸。

²⁸⁵ Germany, Practical Law UK Practice Note (2020 Westlaw)

²⁸⁶ Germany, Practical Law UK Practice Note (2020 Westlaw)

²⁸⁷ Stuttgart Court of Appeal, Court order of 27 November 2020 – 6 W 113/20, GRURRR 2021, 229

²⁸⁸ Stuttgart Court of Appeal, Court order of 27 November 2020 – 6 W 113/20, GRURRR 2021, 229

② 事業を所有していないとの宣言

シュトゥットガルト労働裁判所は、第三者が、不法に取得された営業秘密について、第三者の宣誓の代わりに、もはや事業を所有していないと宣言することを認めた²⁸⁹。

(2) 損害賠償

ドイツ民法の一般規則に従い、損害賠償は、違反行為がなかったかのように、当事者を元の立場に置くために必要な程度で付与される。民法第 249 条に同様の規定が存在している。営業秘密保有者は、営業秘密の侵害から生じた損害を証明するが、計算方法として、失われた利益の補償、侵害者によって得られた利益の引渡し、ライセンスした場合に支払われるべきロイヤルティの支払いが存在する。

なお、ドイツでは、懲罰的損害賠償は採用されておらず、侵害行為が故意か過失かによって額を調整していない。

(3) 暫定的措置

排除措置命令および差止命令は、暫定的措置としても得られる。これらは、UWG の第 8 条に基づき、（ドイツの法律では常にそうであるように）過失又は故意を必要としない。通常、数営業日以内に付与され、一方的な申立手続を経て、暫定的差止命令によって救済を受けうる。

3 公務員による秘密の不正流用

国営企業の従業員が、改修プロジェクトの積算根拠と想定される最大費用に関する情報を漏らした事件に関して、連邦裁判所は、「営業秘密」という用語は、公開入札中に受け取ったオファーにも適用されると判断した²⁹⁰。

4 内部告発と営業秘密の使用・開示

ドイツの脱税事件に関連して、銀行が顧客に関して保有するデータが営業秘密として保護されるかどうか、そのような情報を漏らした銀行員と、そのような情報を使用する税務調査官の両

²⁸⁹ Stuttgart Labour Court of Appeal, Judgment of 18 August 2021 – 4 SaGa 1/21, BeckRS 2021, 26156

²⁹⁰ この特定のケースでは、ドイツの米陸軍地域契約事務所が建設工事契約の公開入札を行っていたとき、一部の米陸軍当局者が、他の競合他社が行ったオファー価格を競合他社に漏らし、それに応じて自分のオファーを調整することができた。5 StR 152/13 (dated 09/04/2013)

方が、UWG 第 17 条に基づいて罰せられるべきかどうかが議論された。同論点は、連邦裁判所によって決定されなかった。

GeschGehG 第 5 条は、違法行為を明らかにするのに役立つ取得、使用、又は、開示が、一般の公益を保護するのに適している場合、取得、使用、又は、開示を、侵害行為から除外する。内部告発は、第 5 条、及び、連合法違反を報告する者の保護に関する指令（EU 2018/0106）の規定に基づき、公益に役立つ限り、刑事責任から免除される可能性がある。

第 5 章 準拠法・域外適用

刑事法の適用に関して、犯罪者がドイツで行動した場合、又は、営業秘密、及び、事業秘密を侵害された企業が物理的にドイツに所在する場合は、ドイツ刑法が適用されうる。

不法行為法の適用に関しては、損害の発生が国内の場合にドイツ法適用がありうる。

GeschGehG の域外適用の可能性に関連する公開された裁判所の決定は見つからなかった。

第 6 章 営業秘密侵害の事件数

営業秘密刑事事件の受理は、フランクフルト支局で、年間およそ 2 桁台前半と報告されているが、公訴や実際の刑事裁判所の判決は殆どない。営業秘密侵害は、詐欺罪等の刑事事件として告発、告訴されるが、捜査、訴追はめったに行われていないとのことである²⁹¹。2015 年の一年間に、営業秘密侵害の刑事事件は 396 件の受理がされたと報告されている。GeschGehG が施行された後、2020 年の一年間で、ドイツ国内の捜査当局に、新法に基づく営業秘密刑事事件として受理されたものは 136 件あったが、訴追は未だ一件もなされていないとのことである²⁹²。

その理由としては、刑事事件として要求される証明の程度が高く、有罪となる見込が少ないと判断されること、証拠収集に時間がかかること、民事で解決されると刑事事件を進行させる意味が失われること、があげられる²⁹³。

なお、ドイツの裁判所による判決や決定は一般的には公開されていない。代わりに、裁判所、又は、いずれかの当事者が、法的に十分に価値がある、又は、公共の利益の観点で重要と見なした場合にのみ公開される。したがって、特定のトピックに関して、公開された判決や決定の数は必ずしも、特定の時間内に下された裁判や決定の総数に対応するわけではな

²⁹¹ Professor Esser インタビュー、Maria von Tippelskirch 氏インタビュー

²⁹² Professor Esser インタビュー

²⁹³ Professor Esser インタビュー

い。また、ドイツの最高裁判所による統計はないようであり、民事事件の総数については不明であった²⁹⁴。

第7章 営業秘密関連の法改正の動き

1 営業秘密法

成立以来、GeschGehG に関する改正は、現在までなされていない。成立した GeschGehG の改正の動きは未だない。

2 デジタル化政策

ドイツ産業連盟が自認するとおり、Digitalization（デジタル化）の分野では、ドイツは EU の先導者としての地位に立てていない。特に、超高速ブロードバンド接続では、遅れがみられる。早急に対応が必要な、サイバーセキュリティとデータ保護に向けて、新しいデジタル技術が産業界に浸透することを目指す必要があることも確認されている。

以上から、ドイツの業界は、企業がデジタル化の可能性を最大限に活用できる環境を開発することを、国内およびヨーロッパの規制当局の両方に奨励している²⁹⁵。

3 サイバーセキュリティ政策

一方、増えつつあるサイバー犯罪による機密情報の漏洩については規制が強化され、基本的な重点化政策が 2021 年に成立している。2021 年 9 月 8 日、連邦内閣は、連邦内務省、建築およびコミュニティ省（Bundesministerium des Inneren, für Bau und Heimat, BMI）によって提示された、新しいドイツのサイバーセキュリティ戦略（2021）、を採用した²⁹⁶。新しいドイツのサイバーセキュリティ戦略は、2016 年のドイツのサイバーセキュリティ戦略に代わるものであり、今後 5 年間の連邦政府のサイバーセキュリティポリシーの基本的な方向性を説明している。

サイバーセキュリティの新戦略の目標は、市民がデジタルテクノロジーを安全に、自由に、そして自己決定的に、使い続けることを可能にすることである。この目標は、特に、高レベルのサイバーセキュリティを通じて、国家、経済、科学、社会のデジタル主権を強化すること、つまり、「個人や機関がデジタル世界で、自己決定的かつ安全に、独立して役割を果たす能力と可能性」を保障することである。

²⁹⁴ Mr. Kuhne 報告

²⁹⁵ Digitalization, BDI. <https://english.bdi.eu/topics/germany/digitalisation/>.

²⁹⁶ Cybersicherheitsstrategie für Deutschland 2021, Kapitel 3 (S. 8).

第1行動分野は、社会の「サイバーセキュリティ能力」を高めるという目標を設定している。たとえば、ITセキュリティソリューションの使いやすさを向上さ、デジタル消費者保護サービスを拡張し、電子IDと電子通信をより適切に保護する。AIをITセキュリティに貢献するツールとして使用することも含めているのが興味深い点である。

第2行動分野は、サイバーセキュリティの分野における、国家、企業、科学、市民社会間の協力の改善によって、国家サイバーセキュリティ評議会の強化、及び、ドイツのデジタル経済とドイツ企業の保護を目指す。

第3行動分野は、危険を回避するための、連邦政府の立法能力と、連邦情報セキュリティ局（Bundesamt für Sicherheit in der Informationstechnik, BSI）と州との間の協力を拡大することを意図する。サイバースペースでの法執行も強化され、セキュリティ当局による、暗号化された通信へのアクセスが作成される。

第4行動分野は、デジタル世代のためのEUのサイバーセキュリティ戦略やネットワークと情報システムに関する指令など、合意された最低基準を導入および実施することを内容とする²⁹⁷。

4 5G 環境の整備

大きな注目を呼んだドイツの5Gのプロバイダー制限に関して、2021年5月7日、連邦議会は、2021年4月23日に連邦議会で可決された、ITセキュリティ法2.0（“IT-SiG 2.0”）を可決した²⁹⁸。連邦議会は、米国のように特定の外国企業を情報通信関係のインフラから排斥する結果となる、排除的な体制を採用することなく、IT-SiG 2.0法案を通過させ、かつ、サイバーセキュリティを含めた国家安全の向上を、重大な政策として遂行する同法を成立させた²⁹⁹。

(1) BSI の権限

連邦情報セキュリティ局（「BSI」）は現在、政府各局と協議し、ITセキュリティに関する拘束力のある最低基準を確立する役割を担っている。現行のITの脆弱性に関する情報を受け取り、影響を受けるITメーカーに報告する、BSIの権限が拡大されると同時に、BSIが

²⁹⁷ これらに伴い、4つのガイドラインの策定が行われており、以下をその内容とする。（1）国家、ビジネス、科学、社会の共同タスクとしてサイバーセキュリティの確立、（2）国家、経済、科学、社会のデジタル主権強化、（3）デジタル化の安全な達成、（4）目標の測定可能化、かつ透明化

²⁹⁸ ドイツ連邦政府、提出された「ITセキュリティ法2.0」の草案（2021年1月27日）
<https://www.bundestag.de/presse/hib/819040-819040>.

²⁹⁹ ドイツ連邦政府、提出された「ITセキュリティ法2.0」の草案（2021年1月27日）
<https://www.bundestag.de/presse/hib/819040-819040>.

情報の受け取りを拒否する権利がないことが明らかになった。

(2) データ保護

IT-SiG 2.0 は、安全性に関わる保存データの保管要件を簡素化した。連邦通信技術の障害、若しくはエラー、または、連邦情報技術への攻撃を、特定、区別、排除するために必要な限りで、ログデータ等が蓄積、収集、および自動的に評価される点には変更がない。IT-SiG 2.0 は、連邦情報セキュリティ局法(BSIG)第5条によるデータの保存期間の制限を、自動評価に必要な期間を超えて、現行のバージョンで規定されている最大3か月から最大18か月に延長した。ただし、BSIG 第5条(3)に従って悪意のあるプログラムが使用されている疑いが確認された際に、悪意のあるプログラムによる危険を回避するために必要な場合、または、他の悪意のあるプログラムを検出して情報技術を保護するため、このデータが使用される実際の蓋然性がある場合にのみ、そのデータ保管が許可される点が、制限として課される。

(3) 製品関連の規制

IT-SiG 2.0 により、BSI には、IT セキュリティの技術ガイドラインを作成するだけでなく、説明する責任があり、同時に、関連する当事者（メーカー、開発者、ビジネス）を含めた、国際標準と標準を考慮に入れ、採用することが明確になった。

2021 年 1 月 25 日の IT-SiG2.0 のバージョンと比較して、IT セキュリティラベル自体に変更はない。IT セキュリティラベルは、1) 製造元の確認、および、2) BSI Web サイトでアクセスできる製品に関する動的セキュリティ情報（リンクまたは電子パッケージ挿入物としての QR コードを介して）の 2 つの要素で構成される。

ただし、IT セキュリティラベルに関連して、IT-SiG 2.0 は、BSI が、IT セキュリティ要件を満たすために、製造元が準拠する必要のある、製品カテゴリーに応じた基準、標準、または IT セキュリティ仕様を、命令で規定することとした。そのような規制がない場合、製造業者は、製品カテゴリーに応じて、BSI によって発行された技術ガイドラインの仕様に準拠する必要があることとなる。

(4) 「特別公益事業」

IT-SiG 2.0 の政府草案は、特別な安全性を必要とする新しいカテゴリーの事業、いわゆる「特別公益事業」を定義した。この例としては、兵器部門の企業のみならず、ドイツ経済にとって重要なものであれば、他の産業、事業も含まれる³⁰⁰。すなわち、サプライチェーン内の事業でも、「独自のセールスポイントのため、公益性の高い事業のサプライヤーとして

³⁰⁰ この点について、草案に関する議論の中で、主管する連邦内務大臣のホルスト・ゼーホーフアーは、ドイツの自動車メーカーに言及している。

本質的に重要である」場合、特別公益事業に該当することとなった。

つまり、これらの事業は、重大なインフラストラクチャと同様の、保護および義務の体制の対象となる。これには、特に、登録、IT 認証、監査、保護対策を含む、2 年ごとの自主的な誓約、および、障害と情報の開示の場合の即時報告が含まれる。

一般に公益性の高い事業に製品やサービスを供給する、サプライチェーンの事業が、特別公益に含まれることになったので、相当に規制範囲が広がった。以上のように、ドイツの特別公益事業へのサプライヤーは、その直接あるいは間接の提供先が、兵器産業や自動車等の事業にあたるのであれば、高度な IT セキュリティの要件を満たし、文書化し、BSI に報告する義務を負うので、今後の対策が必須となる。

(5) 重大なコンポーネント

IT-SiG 2.0 で、「使用がドイツ連邦共和国の治安や治安を損なう可能性がある場合」重要なコンポーネントの使用を禁止できることとされた。そこで、重大なコンポーネントの製造元が、他国の政府によって管理されているか、あるいは、ドイツ連邦共和国、若しくは、他の EU 加盟国の治安や安全に悪影響を及ぼしうる活動にすでに関与しているかどうか、確認されることとなった。5G のサイバーリスクに対処するための、欧州委員会の EU5G ツールボックスのコア要件が考慮される。

5G 通信装置も、この重大なコンポーネントではあり、リスク判定をクリアしなければならない。外務省を含む連邦関係省庁が、製造会社の情報を集め、高リスクの会社については、連邦政府による 5G ネットワークからの排除を可能とする。連邦内務省は、重大なコンポーネントの検討にあたり、使用の潜在的な禁止（事前禁止）を求めることができ、これまでより多くの時間を調査に費やすことができるようになった。

第 8 章 国際協力・他国との連携状況

ドイツは、知的財産権保護制度では EU を主導する加盟国であるが、上記のとおり、ドイツ国内でも営業秘密侵害に関する民事事件はこれまでも存在してきたものの、新法の制定から斬新な変化が見られたわけではなく、また、事件数が急激に増えているとはいえない³⁰¹。

他方、メルケル前首相を継いだオラフ・ショルツ首相は、中国との関係が強いと言われる一方、知的財産権に関しては、自国産業の権利強化を目指すのではないかと見られ、今後の知

³⁰¹ ドイツは、コロナウィルスのワクチンの生産、販売に関して、World Trade Organization's (WTO) intellectual property rules の Waiver をしないことを、他国の求めを拒否して、反対した。

財政策の動向が注目されている³⁰²。

第9章 仲裁の利用

ドイツ国内では、一般事件での仲裁手続の利用も、知的財産権紛争での仲裁手続の利用も、他の EU 諸国に比較すると少なく、進んでいない³⁰³。一方で、特許裁判の利用が圧倒的である。

第10章 ライセンス、生産委託、合併会社設立で気をつけるべきポイント

第一に、EU 指令の内容を取り込んだ GeschGehG 第 2 条が営業秘密として定義するように、「情報を合法的に管理する者によって、当該状況下で、秘密性を保持するための合理的な措置がとられている」ことが要件となったため、機密情報や営業秘密を、秘密保持義務への合意のないまま、第三者に提供することは、それらの「機密性」を失わせる結果となりかねない³⁰⁴。具体的な当事者間の事実関係によらず、法律関係を明確化し、将来の紛争を防ぐためにも、秘密保持義務（守秘義務）を明文で盛り込むことが必要である。

ライセンスを受けるなどして、機密情報あるいは営業秘密を保持する者が、「秘密性を保持するための合理的な措置」を取っているか否かは、以後の営業秘密の保護に重要な事実として関わってくる。秘密保持義務の内容を秘密保持契約書内に盛り込むことも推奨され、契約書に含めるべき項目としては、シュトゥットガルト控訴裁判所が触れた重要な要素がある³⁰⁵。

裁判所の述べたように、必須事項として、従業員が、パスワードによる保護なく自分のハードウェアにファイルを保存することができないことを義務付けているか、また、文書に情報が記載される場合には、無許可の担当者による紙の文書のアクセスを許すなど、秘密情報の管理に失敗することが無いように、（1）ライセンシーにおいて、機密情報、営業秘密を、機密性に関する程度でラベルすること、（2）ライセンシーの従業員の機密性保持の誓約、（3）業務を実行するために少なくとも潜在的に、情報にアクセスすることを必要とする者にのみ

³⁰² Alan Crawford, For Germany's likely new leader Olaf Scholz, Hamburg is at the centre of a growing dilemma over China, Bloomberg (Oct. 23, 2021), <https://www.bloomberg.com/news/features/2021-10-23/germany-s-growing-dilemma-over-china-puts-hamburg-in-spotlight>.

³⁰³ German Arbitration Institute (DIS)での 2020 年の年間仲裁事件数は、165 件であった。うち、外国当事者が関与する事件は半分程度である。 <https://www.disarb.org/en/about-us/our-work-in-numbers>.

³⁰⁴ 第 1 章「営業秘密の定義」を参照。

³⁰⁵ Stuttgart Court of Appeal, Judgement of 19 November 2020 – 2 U 575/19, GRUR-RS 2020, 35613

開示されていること（「知る必要があるベース」）、（4）情報の開示を受ける者は、秘密保持義務に拘束され、情報に関して、この秘密保持義務を負っていることを認識していることを認識していること、などが、プラスの要素となるため、これらの規定を契約書や社内規則等に含めることが推奨される。

本報告書に添付の書式は、前記の重要な要素を含んだ保護措置が採られるように、ライセンシーに義務付けている。ライセンシーの中の誰が機密情報に触れうるかについての特定は、添付文書の形で行われるのが現実的と考えられる。また、相手会社の機密情報を取り扱う者から、個別に、同様の秘密保持契約を取ることも勧められる。

ライセンス、生産委託、合弁会社設立の際に、当事者間で契約書がかわされる場合、契約書に機密保持条項を盛り込むことは通常なされるが、ドイツ法が準拠法である場合には、以下の問題が起こりうるので注意し、ドイツ弁護士に相談するなどすべきである。

1 ライセンス契約

(1) 機密情報、営業秘密の特定

あまりに広範囲で網羅的な条項は、機密性保持の実施が困難であり、実務的ではない。また、技術（に関わる情報）の取引を広げるという、EU の理念とする公共の利益が害されないかが問題とされ得ること、さらに、雇用関係に関連する場合には、被用者の労働の自由が考慮されることも注意すべきである。

実際上は、情報の機密性を示すラベルが有意義と考えられる。機密情報とすべき必要性があること、実際に、機密情報として扱われていることが、後に立証できるよう確認すべきである。

一方、相手会社が、機密情報や営業秘密を利用して生み出すデータや情報を、機密情報や営業秘密に含めることは、多くの場合に、不可能ではないと考えられる。

(2) 機密情報、営業秘密へのアクセス、使用目的、使用方法の限定

契約条項を作成する場合、何が許されるか、そして、何が不正取得、使用、または、開示になるかを明確にすることは、ライセンシー及びライセンサーの利益を守り、また、有効な関係を維持するためにも大切である。例えば、ライセンシー側で、パスワード等アクセス制限を設定すること、アクセスできる者を、一定の被用者、関係会社の被用者、専門家、監査人等に制限すること、アクセスの目的と使用方法を制限することなどが、考えられる。

侵害行為者が、営業秘密の不正使用、開示、取得にあたる事実を認識していたか、認識すべきであったことが、営業秘密侵害の前提とされており、許可事項と不許可事項を分別することが意味を持つと考えられる。

営業秘密保有者において、機密性を保つ合理的な措置をとっていたかどうかを要件として

新たに導入した³⁰⁶。上記のシュトゥットガルト控訴裁判所の判示内容に注意し、パスワード要求、不用意な紙媒体での処理のないことは必須と考えられる。

(3) 契約終了後の情報の返却あるいはデータ削除義務

秘密保持義務の内容として、提供された機密情報、営業秘密は、契約関係終了時に、保有者に返却すること、また、バックアップも含めて、保存されたデータから削除するように要求すること、それを確認すること、を明記することが必要である。これは、前記の機密性を保つ合理的な措置の認定にもプラスの要素として働くと考えられる。

(4) 補償条項

相手方の秘密保持義務違反の結果生じた損害について、相手方に補償の義務を負わせることは、ドイツでも多くの場合に行われている。秘密保持義務条項の有効性が認められる場合、こうした補償条項の効力も同様に認められるであろう。

(5) 損害額

機密情報・営業秘密の保有者は、不正取得、使用、あるいは、開示により生じた損害に対する賠償として、特約がない場合、自分の被った損害を立証して、その填補を求めることができる。ただし、この損害の立証は困難となることが考えられるので、損害額の算定について、事前に合意しておくことも考えられる。

(6) 仲裁合意

裁判による紛争解決と比較し、仲裁は、営業秘密、機密情報の保護に適し、その手続で提出あるいは開示された情報の秘密性が保たれやすいと考えられている。そこで、ライセンス契約にあたっては、仲裁条項を挿入して、仲裁により契約を巡る紛争を解決し、ライセンサーの機密情報や営業秘密の保護を図ることは積極的に検討されるべきである。

なお、仲裁条項は、紛争となった場合の権利保護に対して重要な影響を与える。そこで、疑問のある場合には、国際弁護士に相談することが勧められる。

2 生産委託契約

前掲1 ライセンス契約で列举した注意点は、生産委託契約にも当てはまる。委託者としては、受託者の生産ラインの運営状況、生産品の数量等確認体制、保存・管理状況を十分確認することが特に重要となると考えられる。そこで、契約書にもこれらの事項について、受託者に報告、保証、あるいは誓約をするよう義務づけることは検討されるべきである。

また、生産委託契約では、受託者が、第三者の機密情報、営業秘密情報をたまたま持っていて、委託者の製品の製造に使用してしまった場合、第三者から、機密情報・営業秘密の不正

³⁰⁶ GeschGehG 第2条

使用、開示にあたるとして、請求を起こされてしまう可能性がある。委託者自身が知り得ない場合、委託者に対する請求が認められることはないとしても、暫定措置により生産に対する影響が起こりうる。そこで、生産された製品が、受託者と取引関係のある他社の機密情報・営業秘密の侵害をしないことを誓約する、非侵害保証を要求することは、検討されるべきである。

さらに、機密情報、営業秘密へのアクセス、使用目的、使用方法の限定に関して、受託者から第三者への再委託を禁止することも考慮すべきである。

3 合弁契約

合弁会社は、参加当事者が提供した、あるいは、合弁会社自身が調達した人材、技術、データ、施設、及び、資材を使用して、事業を行うことが多い。参加者の様々な機密情報、営業秘密が提供されることもある。したがって、合弁会社が研究や開発をして得られる成果物に対して、どの者に所有権あるいは管理権が帰属するのかを契約で明確化しておくことは、特に重要となる。

英国

英国と米国は共にコモンローの国であるが、法制度上及び実務上、下記のように営業秘密保護に関して顕著な差異が見られる。

第1章 営業秘密の定義

本章では、現行の営業秘密関連法での営業秘密の定義を、新たに制定された法と判例法のコモンローを比較しつつ説明する。

1 新法による定義

欧州連合議会が、2016年に Directive (EU) 2016/943 (“EU 指令”) を制定したことから、当時欧州連合の加盟国であった英国も、EU 指令の保護内容に応じて、営業秘密の保護を現代化、成文化する作業を開始し、2018年6月9日、The Trade Secrets (Enforcement, etc.) Regulation 2018 (SI 2018/597) (“UK TS 規則”) の制定に至った。ただし UK TS 規則は、すでに存在する判例法のコモンローにより、EU 指令よりも広範囲、あるいは、強力な保護が存在していた場合、営業秘密の保有者は、UK TS 規則の下で付与される保護よりも、コモンローによる拡大された保護を受けられることを明確に記載している³⁰⁷。

UK TS 規則では、営業秘密を次のように定義している³⁰⁸。

- a. 単体として、又は、その正確な構成や要素の組立てに関して、当該情報と同種の情報を通常扱う業界内の人々の間で一般に知られておらず、又は、そのような人々が容易にアクセスすることができない点において、秘密にされている。
- b. 秘密であるために、商業的価値がある。
- c. 当該情報を合法的に管理している者により、特定の状況下で合理的と考えられる、情報を秘密に保つための措置が講じられている。

2 判例法による定義

英国コモンローの衡平法に基づく守秘義務では、関係者間の信頼関係の性状や内容に着目し

³⁰⁷ Robert Williams & Will Smith, Bird & Bird & Trade Secrets (last visited Nov. 21, 2021) <https://www.twobirds.com/~media/pdfs/trade-secrets-article-points-to-note-article-series---sweden---may-2021.pdf>.

³⁰⁸ Trade Secrets (Enforcement, etc.) Regulation 2018 (SI 2018/597) (「UK TS 規則」) 第2条.

て、秘密（営業秘密を含む）が保護されてきた³⁰⁹。裁判例は、情報を秘密とする義務を生じさせる状況で伝えられ、信用関係に由来する情報が、機密情報の保有者にとって不利益に使用され、又は使用の恐れがある場合に、そうした行為を信用に違背する不法行為としてきた³¹⁰。

これに加えて、黙示の信任義務としての守秘義務、忠実義務として守秘義務、明示の守秘義務が生じることがある。

衡平法上の守秘義務で保護を受ける機密情報の内容について、Thomas Marshall (Exports) Ltd v. Guinle 事件では、どのような情報が機密情報にあたるかの判断要素として、以下が挙げられた³¹¹。

- a. 情報は、関係する業界の使用と慣行に照らして、
- b. 行為時に、情報が公開されると、保有者にとって有害である又はライバルにとって有利になる、と保有者が合理的に信じていたか、
- c. 保有者が、情報がまだ公に開示されていないと合理的に信じていたか。

3 新法と判例法の差異

UK TS 規則で規定された営業秘密は、コモンローの衡平法の原理に基づく守秘義務で保護された機密情報の中に含まれると考えられており、保護範囲を拡大するものではないと理解されている³¹²。

實際上、英国裁判所は、第2章及び第4章で述べるように、不正開示、使用、取得行為の判断をするにあたり、事案に応じて、どのような情報をどの程度保護するのか決めている。例えば、当事者間に契約関係が存在し、それが雇用関係の場合、被用者は、雇用者に対して誠実義務や忠実義務を負うことから、雇用者の有する情報を、機密でない情報、機密情報、営業秘密の3つの分類に分け（このうち第3グループの情報が営業秘密と考えられている）、それぞれについて、違法な行為を検討してきた。営業秘密に該当する情報については、契約関係を前提とする忠実義務、誠実義務を前提とすることなく侵害行為が存在しうるので、私的な雇用者の財産的価値の保護、あるいは、不誠実な取引関係の抑止という法益を強化することとなる。

³⁰⁹ 詳しく述べると、営業秘密は、保護される秘密情報のうちの特に機密性の高い情報をさすものとして、裁判例は考えてきたようである。Fraccenda Chicken Ltd v. Fowler [1985] FSR 105.

³¹⁰ Coco v A. N. Clark [1969] RPC 41, 及び Attorney-General v Guardian Newspapers (No 2) [1990] 1 AC 109.

³¹¹ Thomas Marshall (Exports) Ltd v. Guinle [1979] 1 Ch 227

³¹² Clémence Lapotre, Trade Secret Directive Becomes Directly Effective: Growling (June 7, 2018) <https://gowlingwlg.com/en/insights-resources/articles/2018/trade-secrets-directive-becomes-directly-effective/>

第4章で紹介する裁判例において一部説明されているが、コモンローの黙示の守秘義務や衡平の理念に基づく機密情報の保護と、新法による保護は併存するため、実務上、UK TS 規則が大きな変化をもたらすとは期待されていない。しかし、営業秘密法の域外適用の可能性について UK TS 規則がこれを肯定しており、判例法に基づく保護を超えるのではないか、という解釈も現れており、注目されている。

第2章 営業秘密侵害行為

以下で、営業秘密の侵害行為の定義を概説する。

1 新法による営業秘密侵害行為の定義：営業秘密不正取得・開示・使用

(1) 第2条：営業秘密侵害者、営業秘密侵害物件

UK TS 規則の第2条は、「侵害者」とは、営業秘密を違法に取得、開示又は使用した者をいう、と定義している。同条は、「侵害品」とは、営業秘密を違法に取得、使用又は開示した、商品、デザイン、機能、製造プロセス、マーケティング、又は、違法に取得、使用、開示された営業秘密に起因するこれらの有利な特性をいう、と定義している。

他の条文でも、何が「違法に取得、使用又は開示」に該当するかについて、特別に規定していない。したがって、どのような行為が営業秘密侵害行為となるかは、新法は明らかにしていない。

(2) 第3条：保護の拡大

UK TS 規則の Explanatory Note（注釈）は、第3条第(1)項が、どのような営業秘密の取得、開示、使用が違法な取得、開示又は使用となるかは、コモンローの判例法で確立された理論に依拠して決定されることを示している、と注記している³¹³。

(3) まとめ

以上のとおり、営業秘密の侵害行為に関して、新法は、「侵害品」の定義を与えている点で、注目されている。即ち、UK TS 規則が、侵害品自体に対する救済措置を、営業秘密保有者に対して付与しているとの解釈も可能である。しかし、判例法を積極的に変更するような規定は存在しない。

³¹³ UK TS 規則の Explanatory Note.

2 判例法による守秘義務違背の原理：機密情報の不正取得・開示・使用

(1) 伝統的な守秘義務違背：雇用関係に黙示に含まれる守秘義務

英国コモンローの下では、被用者は、雇用者に対して、忠実義務と誠実義務を負うとされている。これらの義務は、雇用契約に伴う黙示の条件であり、契約関係上の義務と理解されている。したがって被用者は、雇用者の秘密を誤用してはならない義務を負う³¹⁴。英国の裁判例では、以下のように、被用者の忠実義務・誠実義務が説明されている。

「法は、被用者が雇用者に対して、忠実にかつ誠実に行動する義務を負うことを、雇用関係に含まれるものとして理解する。被用者は、雇用者が秘密としていることを、業務を行うのに必要とする場合に限りで使用するが、他の目的に使用することはできないという誠実義務を負っていることは、長年に亘って、裁判で支持されている³¹⁵。」

(2) 情報の分類化

現在も英国裁判所によって参考とされる Goulding 裁判官の判決では、問題となった情報の種類に応じて、秘密の使用を3分類に区別し、被用者の情報の使用が、守秘義務に反するかどうか判断すべきと判示した。即ち、従業員がアクセスした可能性のある情報のうち、(i) 最初のグループの情報は、機密ではない情報であり、(ii) 第2のグループは、通常の雇用過程で取得された機密情報であり、従業員の頭の中に残り、彼自身の経験とスキルの一部になる。(iii) 第3のグループは、特定の営業秘密の形式で存在する機密の情報である³¹⁶。第2及び第3のグループの情報は、被用者が、雇用期間中に、雇用されている業務に係る以外で使うことができない義務を負う。しかし、雇用契約の終了に伴い、第2のグループの情報は、このような守秘義務の対象から外れ、被用者は、第3のグループの情報についてのみ、雇用の終了後も開示等してはならないという守秘義務を負う³¹⁷。

(3) 被用者の守秘義務の要素

前記の裁判の上訴審で Neill 裁判官は、従業員が雇用に残っている間は、被用者の黙示の義務として、誠実義務又は忠実義務が課され、従業員の守秘義務もその条件に含まれることを再確認しつつ、次のことに注意を促した³¹⁸。(a) 誠実義務の範囲は、雇用契約の性質によって異なり³¹⁹、(b) 被用者が、雇用終了後に使用するために、まだ雇用されている間に雇用主の顧客のリストを作成したり、コピーした場合、又は、そのような顧客リストを故

³¹⁴ Marathon Asset Management LLP v. Seddon [2017] EWHC 300 (Comm).

³¹⁵ Coco v A. N. Clark [1969] RPC 41

³¹⁶ Fraccenda Chicken Ltd v. Fowler [1985] FSR 105

³¹⁷ Fraccenda Chicken Ltd v. Fowler [1985] FSR 105.

³¹⁸ [1987] Ch 117

³¹⁹ Vokes Ltd. v. Heather, 62 R.P.C. 135.

意に記憶した場合、守秘義務違反となるが、特別な状況を除いて、元従業員が、以前の雇用主の顧客を訪問したり、顧客と取引したりすることについて、一般的に制限はされていない³²⁰。したがって、被用者は、営業秘密に至らないような機密情報については、自分の頭の中にある場合、雇用終了後に開示したり、使用したりしても、忠実義務や誠実義務違反とはならない³²¹。

よって、雇用関係終了後の被用者について、開示、使用が違法な忠実義務、誠実義務違反となるかについては、下記要素を考慮に入れて判断することになる。

- a. 雇用の性質。機密資料が習慣的に取り扱われる地位への雇用は、従業員が、その機密性を認識することが期待できるため、高い機密保持義務を課される。
- b. 情報自体の性質。第3グループの情報（営業秘密）の明らかな例として、製造方法の秘密が含まれる。特定の情報が、限られた人数の者にのみ、限定して配布されているという事実は、情報の性質、その機密性の程度に、重要な示唆を与える。
- c. 雇用主が、情報の重要性、機密性について、従業員に強い認識を植え付けたかどうか。雇用主は、特定の情報について、機密であると従業員に伝えるだけでは、一切の使用又は開示を違法とする営業秘密に位置づけられないが、情報に対する自身の態度が、その情報が第3グループの情報に含まれるのかどうか、判断するのに役立つ場合がある。
- d. 情報を、従業員が自由に使用又は開示できる他の情報から、簡単に分離できるかどうか³²²。

以上のとおり、情報の3分類化、及び、上述の4要素を考慮するというアプローチは、被用者が、雇用契約終了後に別の雇用機会を探し求め、労働に従事する自由を享受することができるという、公共の利益に配慮した判断をするために重要となる³²³。

(4) 被用者の不正取得、使用、開示に関する故意・過失

黙示の契約上の忠実義務、信実義務は、被用者が、情報が機密であることを知っている場合、又は、被用者の立場にある合理的な行為者が知り得た場合にのみ、従業員を拘束するとされている。

³²⁰ Robb v. Green [1895] 2 QB 315 and Wessex Dairies Ltd. v. Smith [1935] 2 K.B. 80

³²¹ Roger Bullivant Ltd v Ellis [1987] FSR 172

³²² Lancashire Fires Ltd v S.A. Lyons & Co Ltd [1996] FSR 629 (CA), at 668-9.

³²³ Vestergaard Frandsen A/S v Bestnet Europe Ltd [2013] UKSC 31; [2013] 1 WLR 1556.

(5) 非公知性、非容易取得性

情報が既に公知となっている場合には、機密情報も、営業秘密も存在しない。

しかし、英国裁判例では、原告から機密情報を不正取得した被告が、当該情報を、他から製品を合法的に入手することで、リバースエンジニアリングで発見する、もしくは、突き止めることができたはずであることと主張しても、機密情報がなかったとすることにはならない。つまり、原告から直接に入手することで、情報を構築するのに雇用者が費やした労働、費用、技術的な困難の克服を省くことができたことで、機密情報の存在を肯定することができる³²⁴。

一部が公開された情報で、他の部分が非公開の機密情報である場合、被用者は、パブリックドメインにある資料のみを使用するように、特別な注意を払う必要がある。つまり、被用者は、公的な情報源から得た場合よりも、有利な立場にあってはならず、雇用者の信用を得て受け取った情報を使って、他人を有利な競争的地位に置くべきでない。ただし、秘密情報に起因する時間と手間を省き、得た価値の多寡によって、差止命令をすることは妥当でなく、損害賠償だけが許される場合も多くあると考えられている³²⁵。

(6) 伝統的な営業秘密侵害行為：衡平法の原理に基づく守秘義務

雇用関係という契約関係に基づく黙示の守秘義務とは別に、衡平法で、信頼関係に由来する信用を基礎として、守秘義務が課せられることがある。つまり、営業秘密などの機密情報を、機密性を保つことに同意した、又は、機密性を認識したか、認識すべきであった状況で受け取った被告が、その機密性と矛盾して使用する場合に、被告による信用の違背と認められる³²⁶。

裁判例では、機密性を認識し得たはずの被告に対して、差止命令を発令することも可能と判断されている³²⁷。

衡平法に基づく守秘義務の場合、契約に基づく守秘義務と異なり、前述の3分類の情報のうち、第2グループの情報については、雇用関係の終了により守秘義務が終わらない。なぜなら、衡平法は、契約関係とは独立して、当事者間の信義、誠実、公平等の観点から、裁判所が義務の有無を決定するものだからである。

(7) 伝統的な営業秘密侵害行為：故意・過失がある第三者による不正取得・使用・開示

³²⁴ Force India Formula One Team Ltd v Aerolab Srl [2013] EWCA Civ 780; [2013] RPC 36

³²⁵ Seager v Copydex (No. 1) [1967] 1 WLR 923

³²⁶ Attorney General v Guardian Newspapers Ltd (No 2) [1990] 1 AC 109, 281.

³²⁷ Primary Group (UK) Ltd v The Royal Bank of Scotland plc [2014] EWHC 1082 (Ch); [2014] RPC 26

原告が、営業秘密等の機密情報を有している場合、競争関係にある被告が、原告の情報を不正に取得したり、使用したりした場合、被告は、原告に対して、衡平法により、直接自己の行為に対する責任を負う。すなわち、被告が、取得した情報が、原告の機密情報で、信用を置いていた者に限定してシェアされていたにもかかわらず、信用違背の結果取得されたことを認識していたか、被告が置かれていた特定の状況下で、合理的な者であればそう認識すべきであった場合には、自己が不正に取得、使用、開示した結果生じた原告の損害について責任を負う³²⁸。

(8) 伝統的な営業秘密侵害行為：新雇用主による不正取得・使用・開示

被告が、原告と契約関係にない場合でも、原告に雇用されていた元従業員を雇用して、原告の営業秘密を巧みに活用することで自己の製品の改良などをした場合、元従業員の違法な守秘義務違背に対して、間接的に責任を負うと判断されてきた³²⁹。被告が、自己の営業に関連して、元原告従業員の不正取得、使用によって利益を受けられたことから、間接的責任である代位責任を負うことになる³³⁰。

あるいは、共同不法行為責任を問えると示唆する見解もある³³¹。

3 新法と判例法の差異

前述のとおり、UK TS 規則は、不正開示、使用、取得行為について、特別に規定しておらず、従来の判例法の法的枠組みが引き続き適用されることとなっている。EU 指令では、営業秘密侵害を認定するための前提として、そもそも営業秘密が存在していたか、さらに、その客観的要件として、保有者が機密性を保つために合理的な措置をとっていたかを独立した要件と打ち立てている。従来の英国裁判例では、機密性の保持のための合理的な措置の存在を独立して考察せず、侵害者が、保有者が当該情報を機密性ある情報として保持し、信用を寄せていた者にのみ当該情報にアクセスさせていたことが明らかな場合に、不正開示、使用、取得を認めていた。UK TS 規則に基づく営業秘密侵害の案件では、これまでのコモンロー下での機密情報の不正開示、使用、取得の案件とは異なり、合理的な措置があったかどうかを、一つの独立した争点として審理する可能性が否定できない。

³²⁸ Vestergaard Frandsen A/S & Ors v Bestnet Europe Ltd & Ors [2013] UKSC 31 (22 May 2013)

³²⁹ Vestergaard Frandsen A/S & Ors v Bestnet Europe Ltd & Ors [2013] UKSC 31 (22 May 2013)

³³⁰ Ocular Sciences Ltd v Aspect Vision Care Ltd (No.2) [1997] RPC 289

³³¹ Growling、脚注 312

第3章 営業秘密侵害に関連する法律、規制の概要

1 営業秘密侵害行為に関する EU 指令及び UK TS 規則

英国が、EU を脱退したことで、EU 指令が、英国裁判所を直接に拘束する効力を持ち続けることはない。他方、UK TS 規則は、EU 指令を英国内法に移行するために誕生したので、営業秘密侵害について規律する UK TS 規則の適用は続く。また、UK TS 規則の適用と解釈にあたって、EU 指令の立法目的、規律内容等が参考とされうる。

(1) 定義規定³³²

前述のとおり、UK TS 規則では、何が営業秘密か、何が営業秘密侵害行為となるかについて定義している。「侵害品」とはデザイン、機能、製造プロセス、マーケティング又は、これらの特性が、不正に取得、使用、又は開示された営業秘密から看過できない程の利益を受けている製品とされている。営業秘密保有者とは、営業秘密を合法的に管理、所持する者を言うことから、ライセンシーも該当することとなる。

(2) 権利・救済手段の期間制限³³³

除斥期間は 6 年とされ、権利の法定期間は 5 年とされている。期間の起算点は、(a) 請求の対象となる違法な取得、使用又は開示が終了する日、(b) 営業秘密保持者が侵害を認識した日のいずれか後の日をいうとされている。

(3) 訴訟（手続）中の営業秘密の保護

関係者又は、手続きの一部を構成する文書にアクセスできる者は、次の要件を充たす営業秘密、又は、営業秘密とされる対象物を、使用又は開示してはならない。

① 利害関係者による正当な理由のある申請、又は、裁判所自身の職権により、命令で、裁判所が機密事項として特定し、

② 手続きへの参加、又は、アクセスの結果として、参加者が知るに至ったもの³³⁴。

また、裁判所は、文書へのアクセスを手続関係者や第三者のうちの一部にのみ限定したり、審理の傍聴・立会いや訴訟記録閲覧を特定の関係者に制限したり、営業秘密を省いたり、塗り潰す等した後の記録を閲覧可能にするといった措置も採ることができる³³⁵。

³³² UK TS 規則 第 2 条

³³³ 第 5 条

³³⁴ 第 10 条

³³⁵ 第 10 条

(4) 恒久的差止命令

- ① 裁判所は、本案の審理により、営業秘密の侵害があったと認めた場合、営業秘密の保有者による申立てに応じて、以下の措置の 1 つ又は複数を命じる恒久的差止命令を発令することができる³³⁶。
- a. 営業秘密の使用、又は、開示の停止、又は（場合によっては）禁止。
 - b. 侵害品の製造、提供、市場への進出、使用の禁止、又はこれらの目的での侵害品の輸入、輸出、保管の禁止。
 - c. 権利を侵害している製品に関する是正措置の採用（適切な場合を含む） -
 - i. 市場からの侵害品の回収。
 - ii. 侵害品から侵害する特徴を失わせること。
 - iii. 権利を侵害している製品の破壊、又は、市場からの撤退。ただし、撤回によって、問題の企業秘密の保護が損なわれないことを条件とする。
 - d. 営業秘密を含む、又は、それを具体化する文書、オブジェクト、資料、実物、又は電子ファイルの全部又は一部の破壊、又は、適切な場合、その文書、オブジェクト、資料、実物、又は電子ファイルの全部又は一部の、申立人への送付。
- ② 裁判所は、上記の恒久的な差止命令について、下記の要素を考慮しなければならない³³⁷。
- a. 営業秘密の価値及びその他の特定できる特徴、
 - b. 営業秘密を保護するために講じられた措置、
 - c. 侵害者による営業秘密を取得、使用、又は、開示する行為、
 - d. 営業秘密の違法な使用又は開示の影響、
 - e. 当事者の正当な利益、及び、暫定措置の付与又は拒否が、当事者に与える影響、
 - f. 第三者の正当な利益、
 - g. 公共の利益、及び
 - h. 基本的権利の保護
- ③ 差止命令を課された侵害者は、以下の場合には、裁判所に対し、差止命令の代わりに、金銭的賠償をすることを申し立てることができる³³⁸。
- a. 申立人が、使用、又は、開示の時点で、違法に使用、又は、開示していた他者から、営業秘密が取得されたことを知らなかった、又は、当該状況下で、知りうるべきではなかった場合、

³³⁶ 第 14 条

³³⁷ 第 15 条

³³⁸ 第 16 条

- b. 当該差止処分の実施が、命令を受けた者に、不釣り合いな損害をもたらす場合、及び
- c. 被害を受けた当事者に賠償することが、合理的に十分できると考えられる場合。

(5) 損害賠償

裁判所は、営業秘密保有者の申立てにより、営業秘密の不正開示、使用、又は、取得が行われていることを知っていた、若しくは、知っているはずであった侵害者に対して、営業秘密の違法な取得、使用、又は開示の結果として被った、実際の損害の賠償を命じる必要がある。裁判所は、a. 又は b. のいずれかに基づいて、損害賠償を与える³³⁹。

- ① 本項に基づいて損害賠償を与える場合、裁判所は、以下を含むすべての適切な要素を考慮に入れる。
 - a. 営業秘密保有者が被った逸失利益、侵害者に生じた不当な利益を含む、引き起こされた経営的影響、及び
 - b. 営業秘密の違法な取得、使用、又は、開示によって、営業秘密の保有者に引き起こされた道徳的偏見を含む、経済的要因以外の要素。
- ② 本項に基づいて損害賠償を与える場合、裁判所は、必要に応じて、侵害者が、交渉によりライセンスを取得した場合に、支払うべきロイヤルティ、又は、手数料に基づいて、損害賠償を与えることができる。

(6) 暫定措置(保全措置)³⁴⁰

- ① 営業秘密保持者の申請により、裁判所は、侵害者とされる者に対して、以下の措置のいずれかを命じることができる³⁴¹。
 - a. 暫定的に、営業秘密の使用、若しくは、開示の停止、又は禁止、
 - b. 侵害品の製造、提供、市場への進出、使用の禁止、又は、これらの目的での侵害品の輸入、輸出、保管の禁止、
 - c. 市場に展開し、若しくは、流通するのを防ぐことができるように、輸入品を含む、侵害の疑いのある製品の押収又は送付。

³³⁹ 第 17 条

³⁴⁰ 第 11 条

³⁴¹ 裁判所は、暫定措置の代わりに、侵害者に、損害額の担保を提供するように命じうる。暫定措置が発令された場合、営業秘密保有者は、裁判所が定めた期間内に本案訴訟を提起しなければならない（提起がされない場合、暫定措置命令を取り消しうるとされる）。第 11 条、第 13 条

② 裁判所は、暫定措置を発令するかどうかの判断にあたり、下記について十分な確信を抱かせることが可能と合理的に見なされる証拠を提供するよう、営業秘密保有者に命じる³⁴²。

- a. 企業秘密が存在する、
- b. 営業秘密保持者が申請を行っており、
- c. 侵害者とされる者が
 - i. 企業秘密を不法に取得した。
 - ii. 営業秘密を違法に使用、又は、開示している、又は
 - iii. 企業秘密を違法に使用、又は、開示しようとしている。

③ 裁判所は、暫定措置の発令をすべきか、及び、その相当性について、恒久的差止命令と同様の要素を考慮しなければならない。

(7) 判決公開における営業秘密を守るための措置³⁴³

営業秘密の違法な取得、使用、又は、開示の訴訟手続において、裁判所は、営業秘密保有者の申立てに基づき、侵害者の費用負担で、判決情報の発信のため、全体的又は部分的公表を含む、適切な措置を命じることができる。裁判所が採る措置は、第 10 条に規定されている営業秘密の機密性を、保持する必要がある。

2 契約関係を基礎とする守秘義務違背

当事者間に、明示に秘密保持契約（あるいは守秘義務条項を含む契約）が締結されていれば、それを根拠として、損害賠償等の請求を行う事が可能である³⁴⁴。他方で、そうした守秘義務を課す契約や条項が、不合理な自由の制約にあたると考えられると、秘密保持契約も条項も、法的拘束力を否定されてしまう³⁴⁵。

明示の守秘義務の他に、第 2 章で述べたように、雇用関係などの法的関係を基礎として、あるいは、コモンローで、黙示の契約上の忠実義務、誠実義務の一内容として、守秘義務が課される場合があり、被用者や会社役員、その他誠実義務の一内容³⁴⁶として生じることがあ

³⁴² 第 12 条

³⁴³ 第 18 条

³⁴⁴ *Marathon Asset Management LLP v. Seddon* [2017] EWHC 300 (Comm)

³⁴⁵ *Marathon Asset Management LLP v. Seddon* [2017] EWHC 300 (Comm)

³⁴⁶ *QBE Management Services (UK) Ltd v Dymoke and others* [2012] EWHC 80 (QB)

る。

3 衡平法下における守秘義務違背

コモンローでは、契約に基づく守秘義務とは別に、衡平法に基づいても、守秘義務が課される。これは、同業者等、保有者と契約関係にないが、保有者の機密情報であると合理的に理解できるような場合に、機密情報を不正に取得した者から買い入れて使用する場合に問題となる³⁴⁷。

4 コンピューター不正使用法

英国裁判所が、1990年のコンピューター不正使用法（Computer Misuse Act 1990）を適用できる犯罪は、下記のような事実、事情がある場合である³⁴⁸。

(1) 第1条：コンピューター装置への不正アクセス

自分のコンピューターを含むコンピューターに、アクセスを確立する目的で機能を実行させる行為。ただし、コンピューターとの単なる物理的接触（操作に至らない行為）、及び、コンピュータープログラムと接触なくデータを閲覧する、あるいは、誰かの出力データを取得する行為は除外されている。したがって、機密情報出力の読み取り、画面に表示されたデータの読み取り、又は、「コンピューターの盗み聴き」（機密情報が表示されている画面を、知りながら敢えて見る）は、いずれも対象外となる。

なお、行為者において、自己にアクセス権がないという認識を有している必要がある。判決で、一部のデータにアクセスできる被用者が、それ以外のデータにアクセスした場合には、本罪が成立するとしたものがある³⁴⁹。

起訴されれば、犯罪に対する罰則は最大2年の懲役とされている。なお、第1条と第2条は、第17条の解釈の条文と併せて検討される必要がある。

(2) 第2条：犯罪遂行目的でのコンピューター装置への不正アクセス

行為者が、さらなる犯罪の実行又は促進を目的として、第1条に基づく不正アクセス罪を実行する場合には、第2条の構成要件に合致し、同条の適用がある。ただし、行為者が意図

³⁴⁷ 前記「営業秘密侵害行為」に掲載の判決を参照。

³⁴⁸ **Computer Misuse Act 1990**

³⁴⁹ **R v Bow Street Magistrates' Court and Allison (AP) Ex Parte Government of the United States of America (Allison) [2002] 2 AC 216,**

した、さらなる犯罪が実際に行われたことを証明する必要はない。

例えば、銀行のコンピューターに不正にアクセスして、電子送金の過程にある資金を、自身の銀行口座、又は共犯者の銀行口座に移行する、窃取の目的で、不正アクセスを取得することが、第2条に該当すると考えられる。又は、情報が関係する人物を恐喝する目的で、コンピューターに保持されている機密情報へ不正アクセスする場合も該当すると考えられている。

第2条の行為に課しうる最大の刑罰は、5年の懲役とされている。

(3) 第3条：コンピューターを誤作動させる目的で、あるいは、誤作動を起こさせるかについて無謀な状況での、コンピューター装置への不正アクセス

第3条(2)項に記載のいずれかを実行することを意図して、コンピューターアクセスが許可されていないことを知って、コンピューター不正アクセスを行うこと、又は、その行為を行うことによって、第3条(2)項に記載の1つが起きるかどうかについて無謀である場合は、本罪に該当する。

例として、意図的又は無謀なコンピューター作動の障害、正当なユーザーによるコンピューター装置へのアクセスの防止又は妨害、又は、コンピューターに保存されている資料の操作又は信頼性を障害することが該当する。行為者は、行為が許可されていないことを認識している必要がある。分散型サービス拒否攻撃(DDoS)を伴う場合、特に、コンピューターの作動、保存内容の改変が起きなくても充足はされ、作動障害は一時的なもので足りる可能性がある³⁵⁰。

DDoSは、さまざまなソースから発信されたトラフィックを使用し、アクセスを集中させることで、インターネットに接続されたホストのサービスを一時的又は無期限に中断し、本来のユーザーが、装置又はネットワークリソースを利用できないようにする一種のサイバー攻撃であり、被害者が、1つのソースだけをブロックすることで攻撃を阻止することができなくする。群衆が事業所の入り口を塞いで、合法的な顧客がアクセスすることを不可能にし、それによって営業を混乱させる手口に例えられてきた。

実際には行為者からのアクセスであるにもかかわらず、別人からのものかのようにコンピューターに情報を記録させた場合、それは明らかにコンピューターの信頼性に影響を及ぼす。したがって、そのような行為は、コンピューターの操作信頼性を損なう第3条(2)項(c)に該当する³⁵¹。

³⁵⁰ DPP v Lennon (2006) 170 JP 532

³⁵¹ Zezev and Yarimaka v. Governor of H.M. Prison Brixton [2002] EWHC 589 (Admin).

ただし、コンピューター上のコンテンツ内容を変更しただけでは、1971 年刑事損害法第 10 条の意味における刑事損害とはみなされない³⁵²。

(4) 第 3ZA 条：重大な損害を与える、又は、そうした危険性を持つコンピューター装置への不正アクセス

不正アクセスをした結果、被害者に重大な損害を与えた場合、行為者は第 3ZA 条により処罰されることになる。特に、人命あるいは国家的安全に影響を与える危険性がある場合、重大犯罪とみなされ、厳しい刑罰が科されることになる。

本罪が適用される場合、最大で 14 年の懲役が科されるが、第 3 条 (a) (b) 項にあたる場合には、無期懲役の法定刑が定められている。

(5) 域外適用の有無

第 1、3、3ZA 条違反の刑事責任は、母国（イングランドとウェールズ）と、少なくとも 1 つの「重要なリンク」があることの証明が必要とされる。重要なリンクには次のものが含まれる。

- a. 被告人が、犯罪時に母国にいる。
- b. 犯罪の標的は母国にある。
- c. 犯罪を助長した技術活動は、母国に拠点を置くサーバーを通過した可能性がある。

5 競争法

競争法は、機密情報や営業秘密を保有する者に救済を与えるというのではないが、機密情報がライバル会社へ提供されることに対して制裁を課すという点では、営業秘密法に無関係なわけではない。

EU の機能に関する条約第 101 条は、EU 内の自由な人的物的移動を保護する規定であるが、反競争的な合意、取決め、協調的行動、慣行を禁止する。また、同条約第 102 条は、市場における支配的地位の濫用を禁止する³⁵³。英国では、1998 年競争法が制定され、同法により、市場取引に影響を与える反競争的協定及び支配的地位の濫用が禁止されている³⁵⁴。

したがって、製品の価格設定や取引業者の選定、あるいは製品の互作用性に関わる技術標準

³⁵² Cox v Riley (QBD) 1986.

³⁵³ The Treaty on the Functioning of the European Union.

³⁵⁴ Competition Act 1998

の決定など、市場における競争に影響を与える可能性のある情報が、その市場に参加している同業者同士で交換される場合、1998年競争法の第1章及び第101条(1) TFEUに該当し、違法となりうる。競合会社間での機密情報の交換が、それ自体が、市場の運営に関して不確実性を軽減又は除去した場合には違法となりえる。なぜなら、市場参加者間の情報交換は、不確実性を低減又は除去することができ、価格競争や技術競争を減殺してしまうからである。

6 刑事営業秘密法

英国では、営業秘密の不正開示、使用、取得自体が犯罪となる旨の特別な刑事法は制定されていない。上述のように、例えば外部者が、営業秘密保有者から許可を受けた者にのみアクセスが許されている、営業秘密を保存しているコンピューターに侵入して、データを盗取した場合には、コンピューター装置不正アクセス法の適用がありうる。

さらに、従業員でも、立ち入りの許されていない施設に立ち入るなどした場合には、不法侵入に関する犯罪が成立し、自己の支配下になく書類や物品の持ち出しがあるのであれば、窃盗法第1条が適用になる³⁵⁵。

7 重複する知的財産権侵害に基づく請求

また、以下のような情報の持ち出しがされ、不法にコピーされて配布されている場合には、著作権法、特許法、意匠法の侵害が問題となることもある³⁵⁶。

- a. 機械工学的デザイン
- b. 製造デザインやモデル
- c. デザインの仕様書
- d. 詳細な技術的情報
- e. 技術的図面
- f. データシート
- g. 操作マニュアル
- h. 説明図や写真
- i. 報告書や見積書
- j. 価格設定表

³⁵⁵ 1968年窃盗法

³⁵⁶ TBD(Owen Holland) Ltd v Simons & Ors [2020] EWHC 30

第4章 営業秘密、機密情報事件の実務（本案裁判例、付随する措置）

1 EU 指令/UK TS 規則による営業秘密保護とコモンローの機密情報保護との関係を問題とした判例

UK TS 規則は、第3条において、UK TS 規則の発効後も、コモンローで衡平の原理に基づいて認められてきた守秘義務違背を請求原因とする請求を行うことができ、それは、UK TS 規則下の営業秘密侵害行為の請求に代えて、あるいは、加えて請求することができる規定としている。

*Trailfinders Ltd. v. Travel Counsellors Ltd.*において、Hacon 裁判官は、これまでに発達した英国の機密情報保護に関する判例法は影響を受けないと判示した³⁵⁷。したがって、Hacon 裁判官は、機密情報及び営業秘密の保護は、市場における競争の促進や被用者の権利など公共の利益とのバランスに配慮する必要があると述べた上、*Faccenda Chicken*が採用した3分類のアプローチにならって、被用者が持ち出した情報がどのような情報にあたるかを吟味し、第2の機密情報にあたりと結論し、機密情報に関わる過去の判例を適用した。

Hacon 裁判官は、機密情報保有者である原告が主張した、元従業員らによる黙示の守秘義務違反、及び、衡平法の守秘義務違反を認定した。更に、被告元従業員らを雇用していた被告会社に対しては、衡平法の原理に基づく守秘義務違反を認定した。他方で、Hacon 裁判官は、被告元従業員らの責任についての被告会社の代位責任は否定した。

2 EU 指令/UK TS 規則による営業秘密保護とコモンローの機密情報保護と両者を取り扱った判例

Celgard, LLC v. Shenzhen Senior Technology Material CO, Ltd では、リチウムイオンバッテリーの生産者で、製法の営業秘密を有している原告が、元従業員であった科学者が被告会社へ転職して、営業秘密に該当する技術を取得、使用したとして、被告元従業員に対しては、コモンローの守秘義務違背を主張し、被告会社に対しては、営業秘密法違反を主張した³⁵⁸。なお、*Celgard*事件では、被告会社が中国の会社であったため、英国で提起された民事事件の被告となった中国会社に対して、相当時間を要する正式な送達によらず、代替的な送達で訴状を送達しうるか、また、英国内で事件を審理することが妥当であるかについて、争われたことから、これらの点へ判断を示した。

被告会社は、被告の製品は被告自身の技術で製造されたもので、原告の営業秘密とは関係ないとし、特に、原告が主張する「営業秘密」があまりに曖昧であり、請求は不合理であり、審理を開始すべきでないと主張した。原告は、自己が営業秘密と考える製法の内容をあまり特定し

³⁵⁷ *Trailfinders Ltd. v. Travel Counsellors Ltd.* [2020] EWHC 591

³⁵⁸ *Celgard, LLC v. Shenzhen Senior Technology Material CO, Ltd* [2020] EWHC 2072

てないことは認めつつ、被告元従業員が被告会社に転職後、被告会社の商品ラインが増加し、商品の製法に基づくと考えられる性能が向上し、市場シェアが増加していることなどの状況証拠に依存し、不正使用があると主張した。裁判所は、原告が主張する営業秘密の特定自体は不十分であるにもかかわらず、状況証拠に鑑み、営業秘密の不正使用の蓋然性は否定できないとした³⁵⁹。

送達に関しての管轄権の有無について、裁判所は、差止命令により禁止される被告の行為が英国内の行為を想定していること、原告が英国内で損害を受けていること等から肯定した。

また、英国で審理することが妥当であるか (Forum Non Conveniens) については、事件で原告の行う請求原因事実だけに限らず、紛争の全体を考慮し、英国外では受けられない救済がないかを考慮しなければならない³⁶⁰と述べて、被告従業員は、米国で雇用されていた後、中国において被告会社に勤務している場合でも、英国内への被告会社商品の流入、英国の顧客の奪取の観点を無視できないことやその他の事情から、英国で審理することは可能であるとした³⁶¹。裁判所は、その判断の中で、準拠法についても検討し、原告が被告らの守秘義務違背により受けた損害は英国で発生していることから、英国法が適用されるとした。

3 機密情報保護の暫定的措置の期間設定、賠償額算定の基礎

デジタルコインのプラットフォームを運営する原告が、退職後に原告を中傷する元ディレクターの被告に対して、機密情報を不正に使用している、あるいは、原告の知名度を不正に使用してなりすましている (Passing-off) などと主張し、被告によるデータベースや顧客情報の不正使用を禁止する暫定的措置を得ていた³⁶²。裁判所は、原告が金銭的賠償を既に請求していること、金銭的損害は、被告の侵害行為がなければ、原告が享受しえたであろう経済的利益を、原告に回復させることを目的としていること、暫定的措置も同様に、原告の損害を填補、回復する目的で付与されることを確認した。争点となった暫定措置の期間について、裁判所は、被告が原告に対して、役員として法律に基づいて信任義務を負っていたことから、一定期間中は原告の機密情報を原告にとって不利になるように使用すべきでないことを肯定したものの、原告が保有していたデータベースや顧客リストを、不正に使用したことがないことを認め、機密情報を不正使用するような被告の意図が明らかでないことを重視し、全体で6ヶ月に限定した。

³⁵⁹ 原告は、証拠保全命令を得たり、コンピューター映像化、検証命令を受けたり、搜索命令を活用したり、文書提出命令を求めることができる。

³⁶⁰ *Re Harrods Buenos Aires Ltd* [1992] Ch 72

³⁶¹ 被告会社の商品は、中国で製造されている可能性は、裁判所も認識していた。

³⁶² *C Wzrd Ltd & Anor v. Kortan & Anor* [2020] EWHC 1360 (Ch).

4 秘密保持契約の効力を否定した例

被用者との雇用契約内に秘密保持義務の規定が存在したが、その規定が、機密情報を網羅的に下記のように定義していた³⁶³。

機密情報とは、機密情報と明記されているか否かにかかわらず、（1）当社が機密情報と考える当社の経営、顧客、製品、事務、並びに、財務に関する（経営展開プラン、価格設定、研究や解析結果を含むが、それに限らない）情報、及び、（2）当社の経営、並びに、供給者、顧客、代理人（中略）のいずれかに関する技術的データ、ノウハウを含めた営業秘密をいう。

あなたは、雇用に伴い、機密情報にアクセスすることがある。あなたは、雇用中と雇用終了後も、自分の職務の適切な遂行以外に、機密情報を使用、若しくは、いかなる人、会社、他の団体にも開示しないことを合意する。

裁判所は、このような限定のない条項は不当な自由と競争の制限にあたり、法的拘束力を持たないと、傍論で結論した。

5 暫定措置の内容を複数の期間に分割して、異なった内容の秘密保持措置を命じ、擬制信託を否定し、秘密保有者の「汚い手」について言及した例

従前より、雇用者等の営業秘密保有者が、以下で説明するような、製造や販売等の差止命令、証拠提出命令、収支の報告命令、被告の営業利益の擬制信託への吸収等、強力な（暫定又は恒久的）措置を、競争相手や元従業員に対して発動し、決定的なダメージを与えることができることの問題は認識されてきた。そこで、既に現状維持のための差止命令が発令されている場合には、それに加えて、被告の製品を原告や中立的な保管者へ送付すべきとする命令は不要、と結論する裁判例が存する³⁶⁴。

擬制信託とは、当事者間に信託契約が無いにもかかわらず、自己の違法な（大抵の場合には、原告の信頼を裏切るような形でなされる）行為に直接的に由来して、利益を得ている被告に対し、あたかも信託の受託者の忠実・誠実義務を負っているかのように考えて、被告の営業活動の内容について、原告に報告させるとともに、収益を自己の財産とは分離して、確実に管理さ

³⁶³ Quilter Private Client Advisers Ltd v. Falconer & Anor [2020] EWHC 3294.

³⁶⁴ Ocular Sciences Ltd v Aspect Vision Care Ltd (No.2) [1997] RPC 289

せるという措置を課すものである³⁶⁵。英国の裁判例で認めたものもあるが、積極的に擬制信託を課すことは妥当ではないのではないか、という意見が強い³⁶⁶。

また、営業秘密保有者が自己の顧客に対して、裁判所が実際に与えた救済措置以上に命令があるかのように誤導するなどして、不正な行為を行った場合には、そのような行為が救済の否定につながることを示唆した。具体的には、既に存在する暫定措置による制約で守られる利益が十分なことも考慮しつつ、営業秘密保有者が求めうる内容を制限的にのみ認容した³⁶⁷。

6 暫定的措置

(1) 一方的申立て（非対審式）

暫定的申立ての多くが、まずは営業秘密保有者が一方的な(ex parte)暫定的措置の発動を求めることから始まるため、機密情報や営業秘密を侵害するような被申立人の行為の差し止めを求め、被申立人が参加せず、対審構造をとらない手続で決定に至ることが多い³⁶⁸。これには、営業秘密保有者にとって非常に迅速な救済が得られるというメリットがある反面、制度が濫用される恐れがある。一つの対策として、申立人は、被申立人が被る可能性のある損害を担保するため、担保を預託しなければならないとされている。

以上とは別に、より幅広い、あるいは、より強力な暫定的措置の申立てに関しては、被申立人の参加を許した後に決定に至るという段階を得て発せられる³⁶⁹。

(2) 暫定的差止命令の要件

裁判所は、暫定的差止命令申立において、下記の事項を考慮して、措置を命じるかどうか決定する³⁷⁰。

- a. 本家で審理されるべき重要な問題がある（申立人が勝訴する合理的な可能性がある）
- b. 本家が解決するまで待てない緊急の必要性を申立人が有する（金銭的賠償に代えられない利益）
- c. 申立人と被申立人の被る困窮度の比較
- d. 現状が維持されなければならないとする要素の存在³⁷¹

³⁶⁵ Ocular Sciences Ltd v Aspect Vision Care Ltd (No.2) [1997] RPC 289、Spycatcher case [1990] AC 109 参照。

³⁶⁶ Ocular Sciences Ltd v Aspect Vision Care Ltd (No.2)

³⁶⁷ Fortescue Metals Group Ltd & Anor v. Argus Media Ltd & Anor [2020] EWHC 1304 (Ch).

³⁶⁸ Huw Evans, et al., Trade Secret Protection: the regimes in key jurisdictions (2017)

³⁶⁹ Forse and others v Secarma Ltd and others [2019] EWCA Civ 215

³⁷⁰ Forse and others v Secarma Ltd and others [2019] EWCA Civ 215

³⁷¹ American Cyanamid Co v. Ethicon Ltd [1975] AC 396

(3) 暫定措置の内容

暫定措置の内容として最も基本的なのは、被申立人による機密情報の不正な使用、開示、取得（譲渡しと譲受け）の禁止である。この他にも、下記のようなことを命じる決定がなされうる。

① 搜索と押収命令

1975 年、*Anton Piller KG v Manufacturing Processes Ltd & Ors* 事件において、英国裁判所は、申立人が被申立人の事業敷地内に赴いて、不正取得、使用の決定的証拠となる文書の搜索と押収ができる旨の命令を下した³⁷²。申立人である Anton Piller KG は、被申立人が機密情報を不正に開示しており、技術的図面及び手順書を著作権を侵害してコピーしていると主張した。申立人は、一方的な審理手続きで、被申立人の敷地に立ち入り、関連文書を検証し、押収することを許可するよう裁判所の命令を求めた。下級審は却下したが、上級審の Omrod 裁判官は、次の要件下に、申立てを認めることとした。

- a. 申立原因事実について、格別に強固な立証があること、
- b. 予測される、又は、現実の損害が、申立人にとって、非常に重大であること、
- c. 被申立人が、その手中に、侵害の事実を明らかにする文書や物体を所持しており、もし、被申立人に手続きへ参加させる審理をすると、それら資料を破壊する現実的恐れがあることを明白に示す証拠がある。

この搜索と押収命令は、被申立人に通知をしないで、決定を得られる点で、営業秘密を保有する申立人に有利であるため、頻繁に利用されるようになった。他国でも（オーストラリア、カナダ、香港、インド、アイルランド、イスラエル、ニュージーランド、南アフリカ）裁判所は、この方式を採用した。さらに、搜索と押収命令は、機密情報たる物やデータそのものが被申立人の管理下にある場合、これら機密情報を取り戻すためにも使用されている³⁷³。

② 資産凍結命令

侵害者が、比較的弱小な法人で、経営状況が不安定である場合、若しくは、資産隠しをする可能性がある場合など、申立人は、被申立人の財産が処分又は変動しないようにする、資産凍結の命令を求めることができる³⁷⁴。要件としては、

- a. 申立原因事実について、一応の立証がある、

³⁷² *Anton Piller KG v Manufacturing Processes Ltd & Ors*, [1976] 1 All ER 779, [1975] EWCA Civ 12, [1976] Ch 55.

³⁷³ *Yousif v Salama and Another* [1980] 1 WLR 1540

³⁷⁴ Huw Evans、脚注 368

- b. 資産が減少する恐れがある、
- c. 被申立人が、裁判所の管轄地内に、資産を有している。

本命令も、被申立人にとって致命的な打撃を与える可能性があるため、より緩やかな手段で目的を達成できないかを検討する。

③ 証拠保全命令

証人審問が終了するまで、証拠を滅失させたり、変造したり、性質を変えるなどを禁止する³⁷⁵。

④ 送付命令

被申立人に対し、いくつかのカテゴリーの情報を申立人に提供させることを命じる。被申立人は、申立人がコンピューターフォレンジックを用いて情報を解析できるような形態で、これを提供しなければならない³⁷⁶。

また、被申立人に対し、機密情報の侵害（不正な取得、開示、又は、使用）の結果により作られたと疑われる製品を、申立人が吟味できるように、申立人の指定する場所へ送付すべきことを命じることも可能な場合がある。

⑤ 報告命令

被申立人が機密情報を不正に使用して、申立人の技術を実装した製品を製造したり、顧客を得ている疑いのある場合、被申立人の関連する事業の収支について報告させるものである。

第5章 域外適用

以下は、営業秘密保護法の域外適用についてであるが、英国の欧州連合離脱を念頭として、法制度、裁判例を説明する。

上述のように、コンピューター不正使用法 UK TS 規則は、EU 指令を英国内法に移行、実施するために、第2条において、「営業秘密」、「侵害行為」、「侵害品」に関して定義を設けた³⁷⁷。そこで、機密情報の不正な開示、取得、使用に対するコモンローの保護とは異なる地理的保護範囲を議論する余地が生じた。

EU 指令/UK TS 規則の域外適用を問題とした裁判例には、*Celgard, LLC v. Shenzhen Senior Technology Material Co.* があり³⁷⁸、下記のように、重要な判示がなされた。営業秘密の実際

³⁷⁵ Huw Evans、脚注 368

³⁷⁶ Huw Evans、脚注 368

³⁷⁷ UK TS 規則第2条

³⁷⁸ *Celgard, LLC v. Shenzhen Senior Technology Material Co Ltd* [2020] EWHC 2072

の取得や営業秘密を使用した商品の製造は、英国外でなされている。

原告は、被告らの守秘義務違反により受けた損害は、輸入先である英国で発生しており、英国の不正な競争に関して生じる請求が問題となっているので、英国法が適用されると主張し、被告は、中国法が適用されると反論した。下級審は、原告の求める、被告会社製品の英国内への輸入の差し止め等の請求に、中国の裁判所が中国法を適用する可能性は低いと、専門家証人が結論していることから、英国法が適用されると認めた。

上級審(Arnold LJ, Popplewell LJ と Davis LJ が同意) は、EU 指令第 4(5)条の解釈を議論し、下級審の結論を支持した³⁷⁹。

第6章 営業秘密、機密情報の事件数（本案裁判例）

営業秘密事件の民事事件数の概要、刑事責任訴追状況を述べる。

1 刑事

営業秘密侵害罪がないため、刑事事件は存在しない。

2 民事

民事事件については、EU 指令を受けて UK TS 規則が制定され、営業秘密侵害自体を保護する法律が誕生したことから、事件数は今後増加していくのではないかと考えられる。しかし、UK TS 規則施行後の、公開されている裁判例では、営業秘密を扱った民事事件（2020 年 1 年間）は、全英国で 14 件、機密情報で 20 件に過ぎなかった³⁸⁰。これは、UK TS 規則施行直後であることが関係している可能性がある。

しかし英国では、これまでも、本案訴訟となる営業秘密事件も機密情報事件も非常に少なかった。それには、以下のような理由が考えられる³⁸¹。

まず、機密情報も営業秘密も、知的財産権とは認められておらず、契約に基づく関係や衡平法などの、当事者間の関係と切り離して考えることは難しいことから、契約にまつわる事実や当事者のインタラクションが紛争の鍵となり、かつ、請求の原因となる。

³⁷⁹ とりわけ、パラグラフ 3 が、「営業秘密を違法に取得した」と規定し、取得が「違法」であったかどうかの問題にどの法律を適用すべきかという問題を未解決のままにしていると認めた。したがって、これはやがて CJEU が回答する必要があることを認めた。Shenzhen Senior Technology Material Co Ltd v Celgard, LLC (Rev 1) [2020] EWCA Civ 1293.

³⁸⁰ Bailii ウェブサイトの事件検索結果 https://www.bailii.org/form/search_cases.html.

³⁸¹ Mr. Williams 氏のインタビュー

また、申立てにより、侵害者に対する暫定的措置が発せられた場合、かなり多くの場合で紛争は解決するので、本案事件の提起も必要がない。

よって、比較的訴訟数の少なかった英国での、営業秘密を含む機密情報に関連する法はこれから進展する可能性がある。刑事罰の立法化も、全く可能性がないとは言えないが、表面化はしていない。

第7章 営業秘密関連の法改正

営業秘密に関連した法改正の動向であるが、上記のように、営業秘密に関する新法であるUK TS 規則は、2018年に誕生しており、現時点では、さらなる国内法改正の動きがない。

なお、Brexit後のUK-EU間の知的財産権関連の条約締結の動きであるが、House of Lordsによる調査報告では、Draftの条約では、営業秘密の保護は特に変更が無いであろうとされている³⁸²。

第8章 国際協力・他国との連携状況

以下で、英国政府による、営業秘密保護のための他国との連携について述べる。

英国は、EUを脱退しているが、EU指令に基づいた国内法を制定しているため、EU諸国の営業秘密保護と同レベルの保護は確保されている、という認識が一般である。英国のCustoms & Borderにおける営業秘密侵害品の押収は、他のEU諸国と同様に、非常に難しいとされている³⁸³。これは、営業秘密侵害品に限らず、特許侵害品についても同様である。なぜなら、税関職員には、侵害品であるかどうかを容易に判断する能力がないためである。したがって、営業秘密保有者が税関職員に請求するなどして、侵害品の押収を委託することは期待できないと考えられている。

前述のとおり、英国の裁判所は、米国で不正に取得され、中国等で不正に使用されている営業秘密の侵害事件について、英国に輸入されようとしている場合に、機密情報の侵害行為に対する管轄を肯定した³⁸⁴。また、米国で本案が係属している事件について、たまたま侵害者が英国内に資産を有していた場合、被告の資産を凍結する命令を出した事件もある³⁸⁵。

³⁸² Professor Phillip Johnson, Professor of Commercial Law, Cardiff University (PBS0013) (June 22, 2020) <https://committees.parliament.uk/writtenevidence/7567/default/>.

³⁸³ Professor Phillip Johnson、脚注 382

³⁸⁴ Celgard, LLC v. Shenzhen Senior Technology Material CO, Ltd [2020] EWHC 2072

³⁸⁵ Motorola v. EWHC

第9章 仲裁の利用

一般に、仲裁手続は、裁判所における訴訟と比して、当事者が有する営業秘密や機密情報の秘密性が保たれると言われる。確かに、英国の仲裁機関で仲裁を行う場合、当事者も仲裁人も、仲裁の内容について口外しないという秘密保持の義務を負うと理解されている³⁸⁶。したがって、仲裁合意がある限り、営業秘密が問題となる事件では仲裁の利用が望ましいとも考えられる³⁸⁷。

WIPO の事務局によると、営業秘密関係事件の仲裁事件は、近時増加の傾向が見られるとのことであった³⁸⁸。これは、営業秘密を会社の知的財産権の一部あるいは周辺に位置づける実務にも由来するであろう。他の英国内の仲裁機関では、営業秘密事件数は公表されていない。

第10章 ライセンス、生産委託、合併会社設立で気をつけるべきポイント

以下、ライセンス、生産委託、合併会社設立で気をつけるべきポイントを説明する。

第一に、機密情報や営業秘密を、秘密保持義務への合意のないまま第三者に提供することは、それらの「機密性」を失わせる結果となりかねない³⁸⁹。当事者間の契約関係に由来して、黙示の（機密情報及び営業秘密の）守秘義務を生じさせることがあることは以上に見たとおりであるが、ライセンス契約はそのような守秘義務を生じさせる契約関係として捉えられていない。また、衡平法の原理に基づく守秘義務は、具体的な事実関係に依存し、どのような状況で生じるかはっきりしないことが多いので、当事者間の法律関係を明確化し、将来の紛争を防ぐためにも、秘密保持義務（守秘義務）を明文で盛り込む必要がある。

ライセンス、生産委託、合併会社設立の際に、当事者間で契約書がかわされる場合、契約書に機密保持条項を盛り込むことは通常なされるが、英国法が準拠法である場合には、以下 1. ～3. のポイントに注意し、必要に応じて英国弁護士に相談するなどすべきである。

³⁸⁶ Nikki O'Sullivan, *Keeping it under wraps: the limits on confidentiality in arbitration* (2017), <http://arbitrationblog.practicallaw.com/keeping-it-under-wraps-the-limits-on-confidentiality-in-arbitration/>.

³⁸⁷ しかし、秘密保持は全能ではない。仲裁判断は、後に裁判所で争われることがあるためである。O'Sullivan、脚注 386

³⁸⁸ WIPO, Symposium "Thinking Internationally About IP and ADR: What Every Lawyer & Corporate Counsel Should Know Virtual Seminar" hosted by the University of Illinois System (Aug. 19, 2021).

³⁸⁹ 前記「営業秘密の定義」を参照。

1 ライセンス契約

(1) 機密情報、営業秘密の区別

上述のとおり、英国では、機密情報と営業秘密は区別され、例えば、自己商品に内在する不具合に関して集められた情報は、機密性ある情報とは言えようが、営業秘密には該当しないと判断される可能性もある。ライセンス交渉にあたり、何が営業秘密にあたりうるかは十分に検討する必要がある。

(2) 機密情報、営業秘密の特定

第4章で紹介した判例のように、あまりに広範囲で網羅的な条項は、効力を否定されることがある（公正な競争の保持という公共の利益が、害されないかが問題とされる。また、当該事例のように、雇用関係に関連する場合、特に、被用者の労働の自由が考慮される）³⁹⁰。

実際に、ライセンシーにおいて機密情報が一体何なのか判別できない状況で、ライセンサーから情報を受け取っても、十分に保護のしようがない。機密情報とすべき必要性があることと、実際に機密情報として扱われていることが、後に争点となり、審査されるのであり、機密情報・営業秘密を明確に特定し、秘密性に配慮した受渡しをすることが非常に重要となる。

(3) 機密情報、営業秘密へのアクセス、使用目的、使用方法の限定

契約条項を作成する場合、何が許されるか、そして、何が不正取得、使用、又は、開示になるかを明確にすることは、ライセンシー及びライセンサーの利益を守り、また、有効な関係を維持するためにも大切である。例えば、ライセンシー側で、パスワード等アクセス制限を設定すること、アクセスできる者を制限すること、アクセスの目的と使用方法を制限することなどが考えられる。

衡平法上の守秘義務違背には、行為者が機密情報の不正使用にあたることを認識していたか、認識すべきであったことが、前提とされており、許可事項と不許可事項を分別することが意味を持つと考えられる。

また、新法である UK TS 規則は、営業秘密保有者において、機密性を保つ合理的な措置をとっていたかを要件として導入した。³⁹¹未だ判例法として確立はしていないものの、ライセンサー内部で機密性保持がどのように実施されるべきかは逐次検討し、不十分な点は是正すべきである。

³⁹⁰ Quilter Private Client Advisers Ltd v. Falconer & Anor [2020] EWHC 3294.

³⁹¹ UK TS 規則第2条

(4) 契約終了後の情報の返却あるいはデータ削除義務

秘密保持義務の内容として、提供された機密情報、営業秘密は契約関係終了時に、保有者に返却すること、また、バックアップも含めて、保存されたデータから削除するように要求すること、それを確認すること、を明記することが必要である。これは、前記の、機密性を保つ合理的な措置の認定にも、プラスの要素として働くと考えられる。

(5) 損害額

機密情報・営業秘密保有者は、不正取得、使用、あるいは、開示により生じた損害に対する賠償として、特約がない場合、自分の被った損害を立証して、その填補を求めることができる。この損害の立証は、営業秘密侵害行為の立証や損害の特定と関連して、困難となることも考えられるので、損害額の算定について、事前に合意しておくことも考えられる。

(6) 仲裁合意

裁判による紛争解決と比較し、仲裁は、営業秘密、機密情報の保護に適し、手続きで提出あるいは開示された情報の秘密性が保たれやすいと考えられている。そこで、ライセンス契約にあたっては、仲裁条項を挿入して、仲裁により契約の紛争を解決し、ライセンサーの機密情報や営業秘密の保護を図ることは、積極的に検討されるべきである。

2 生産委託契約

上記に列挙した注意点は、生産委託契約にも当てはまる。

委託者としては、受託者の生産ラインの運営状況、生産品の数量等確認体制、保存・管理状況を十分確認することが特に重要となると考えられる。そこで、契約書にも、これらの事項について受託者に報告、保証、あるいは誓約をするよう義務づけることは検討されるべきである。

生産委託契約では、受託者が、第三者の機密情報、営業秘密をたまたま持っていて、委託者の製品の製造に使用してしまった場合、第三者から、機密情報・営業秘密の不正使用、開示にあたるとして、請求を起こされてしまう可能性がある。委託者としては知り得ない場合にも、「侵害品」に対する救済は与えられているので、影響を受けることとなる。そこで、生産された製品が、受託者と取引関係のある、他社の機密情報・営業秘密の侵害をしないことを誓約する、保証を要求することは、検討されるべきである。

機密情報、営業秘密へのアクセス、使用目的、使用方法の限定に関して、受託者からの再委託を禁止することも考慮すべきである。

3 合弁契約

合弁会社は、参加当事者が提供した、あるいは、合弁会社自身が調達した人材、技術、データ、施設、及び、資材を使用して事業を行うことが多い。参加者の様々な機密情報、営業秘密が提供されることもある。

したがって、合弁会社が研究や開発をして得られる成果物に対して、どの者に所有権あるいは管理権が帰属するのかを契約で明確化しておくことは特に重要となる。

第1章 米国における参考書式	127
1 就業規則における秘密保護関連規定の例	127
(参考和訳)就業規則における秘密保護関連規定の例	132
2 従業員との秘密保持契約書の例	137
(参考和訳)従業員との秘密保持契約書の例	141
3 退職後の競業避止契約書の例	144
(参考和訳)退職後の競業避止契約書の例	147
4 取引先との秘密保持契約書の例	150
(参考和訳)取引先との秘密保持契約書の例	154
5 来訪者受付表	157
(参考和訳)来訪者受付表	158
 第2章 ドイツにおける参考書式	 159
1 就業規則における秘密保護関連規定の例	160
(参考和訳)就業規則における秘密保護関連規定の例	170
2 従業員との秘密保持契約書の例	182
(参考和訳)従業員との秘密保持契約書の例	185
3 退職後の競業避止契約書の例	186
(参考和訳)退職後の競業避止契約書の例	189
4 取引先との秘密保持契約書の例	191
(参考書式)取引先との秘密保持契約書の例	197
5 来訪者受付表	200
(参考和訳)来訪者受付表	201
 第3章 英国における参考書式	 202
1 就業規則における秘密保護関連規定の例	203
(参考和訳)就業規則における秘密保護関連規定の例	239
2 従業員との秘密保持契約書の例	253
(参考和訳)従業員との秘密保持契約書の例	259
3 退職後の競業避止契約書の例	265
(参考和訳)退職後の競業避止契約書の例	269
4 取引先との秘密保持契約書の例	273
(参考和訳)取引先との秘密保持契約書の例	280
5 来訪者受付表	287
(参考和訳)来訪者受付表	288

第1章 米国における参考書式

1 就業規則における秘密保護関連規定の例

Trade Secret Policy

Scope

This policy sets forth procedures and measures to protect information identified as trade secrets owned by Company entities that shall affect all Company employees (herein, employee includes part and full time; temporary and permanent) and contractors.

Policy

1. Trade Secret Definition

A trade secret is information that is kept secret and provides economic value or a competitive advantage to Company because of its status as secret. Examples of information that could be considered a trade secret include information such as, but not limited to, formula, pattern, algorithm, compilation, program, method, technique, customer lists, data sets or compilations, product road maps, pricing schedules, failed experimentation, or manufacturing processes.

Information qualifying as a trade secret shall be identified as such by Company's Intellectual Property (IP) committee and those employee(s) authorized to access the trade secret shall be responsible for maintaining its secrecy.

Factors that weigh into the consideration as to whether information should be considered a trade secret or Company confidential information or alternatively protected under other forms of IP are as follows:

- extent the information is known outside the business
- extent the information is known inside the business
- extent of measures that are used to guard the secrecy of the information
- ease or difficulty to reverse engineer
- value of the information to company and competitors
- effort/cost to develop information

In certain jurisdictions, the trade secret needs to be continuously used in the business.

2. On-Boarding Acknowledgement and Employment Agreements

- a. At some point during the on-boarding process, an employee or contractor shall acknowledge that they will not use or disclose the trade secrets, inventions, and other proprietary and confidential information belonging to third parties. An acknowledgement form regarding third party trade secrets and proprietary information will be provided.
- b. Before the employer/employee or employer/contractor relationship begins or meaningfully changes (e.g., by a promotion or assignment change) and before any trade

secrets are disclosed, the employee or contractor shall sign an agreement that includes at least the following:

- i. **IP Assignment:** Every employee or contractor shall sign an IP assignment. The agreement shall include a present assignment expressly transferring to the Company as the owner of IP, IP including trade secrets, developed by the employee during and in connection with his or her employment. A similar assignment also shall be signed by consultants, licensees, or other third parties where applicable.
- ii. **Confidentiality Provision:** Every employee or contractor shall sign a Confidentiality Agreement acknowledging their duty of confidentiality with respect to Company's information and trade secrets. A similar agreement also shall be signed by consultants, licensees, or other third parties.
- iii. **Non-Compete/Non-solicitation:** To the extent permitted by law, the agreement shall contain provisions prohibiting an employee or contractor from accepting employment or performing services for a competitor or competing with Company or soliciting a former employer's customers or employees.

For additional information, please consult the *Employee Handbook* and/or Human Resources (HR).

3. Third Party Agreement

Prior to entering a contractual relationship with a third party, a non-disclosure agreement (NDA) or agreement containing confidentiality provisions shall be executed before any Company confidential information -particularly trade secret information- is shared. **If trade secrets are to be shared with third parties, kindly alert the Legal Department so additional contractual provisions may be included in the NDA or other agreement for added protection.**

4. Physical Security Measures

- a. **Facility Security Measures:** Access into and out of the facility shall be controlled and monitored with visitor sign-in logs with picture ID required, visitor non-disclosure agreements (NDA's), pre-approval of all visitors, and surveillance cameras. All visitors shall be accompanied by an escort while on-site and are prohibited from on-site use of any device with recording capability (e.g., camera, video-camera, stop-watch or smart-phone with any of those functions).
- b. **Restricted Access:** Access to the building shall be restricted through locked doors requiring badge entry issued to only authorized employees and contractors. All physical embodiments of a trade secret, whether a prototype, working model or actual embodiment in use, shall be maintained in a restricted area that is under lock and key and out of view. Employees or contractors shall put working materials or files containing trade secrets in a locked desk or filing cabinet when not in use (see *Clean Desk Policy*).

5. Marking

A trade secret shall be conspicuously marked as strictly confidential per our Global Marking Policy. This marking shall differentiate the trade secret information from other Company confidential

information. Accordingly, for trade secret information all physical documents and digital files shall include “Company Strictly Confidential” either in the form of a header, footer or watermark. In any instance where trade secret information can be copied or downloaded, such copying of such document or digital files is tracked, monitored, and destroyed after use.

6. Trade Secret Storage

- a. **Identification and Description of Trade Secret:** Once information has been identified as trade secret, the Company IP attorney will prepare a brief description of the trade secret.
- b. **Protective Measures:** Trade secrets will be maintained and protected in a manner that is greater than that of Company confidential information. All trade secrets shall be stored in a trade secret database on a Company controlled network that is password protected where the password is known only to Authorized Persons (defined in Section 7 herein). Additional encryption measures may be used where appropriate. The database shall be maintained by a Company IP attorney and/or Information Technology (IT) where access is granted. Trade secrets shall be segregated from other Company confidential information and only accessible through a Company-controlled network and not through any other network, cloud storage, or the internet except via the Company Internal Private Network (VPN). Old hardware, such as laptops or hard drives containing trade secret information, should be physically destroyed rather than being thrown away or recycled.

7. Limited, Need-to-Know Access

- a. **Responsible Employee:** Employee(s), as designated by a Company US IP attorney or the Company IP committee, shall be responsible for maintaining the secrecy of each trade secret by ensuring that the requirements of this policy are met for that trade secret.
- b. **Authorized Persons Only:** Access or use of a trade secret by an authorized person is authorized only if, and only to the extent, he or she needs to access or use the trade secret to perform his or her job responsibilities. An authorized person may copy a trade secret, or a portion of a trade secret, only if necessary, to perform his or her job responsibilities. All such copies shall be promptly destroyed, i.e. rendered indecipherable and unable to be reconstructed once they are no longer needed.
- c. Visitors must sign acknowledgments prohibiting disclosure of information viewed or accessed during a visit, preventing them from bringing recording devices (e.g., cameras, cell phones, USB drives) into restricted areas, and requiring that they be accompanied by employees while in locations where they may access sensitive information.
- d. **Electronic Information Management:**
 - i. Access to trade secrets shall be limited to only authorized persons and through only authorized means.
 - ii. If information relating to a trade secret must be shared between authorized persons, it shall be done through secure transfer means, i.e. via encrypted email or a secure file transfer.
 - iii. A list of the persons authorized to access a trade secret shall be maintained by the Responsible Employee for each trade secret and/or the Company IP Attorney.

8. Protected Networks and Mobile Devices

- a. **Network and Device Security:** Network and device security solutions shall be maintained by Company's IT department as in the normal course of business.
- b. **Personal Devices:** Employees and contractors shall follow Company's policies regarding use of company devices that precludes employers and contractors from using personal devices for work related matters unless he or she has complied with Company's *Bring Your Own Device (BYOD) Policy*. **Downloading or use of trade secret information on personal devices is prohibited.**
- c. **Portable Device or Drives:** Portable devices or drives are not allowed for use on Company computers.

9. Proprietary Data Control

All presentations, articles, and research papers that are to be publicly disclosed, or otherwise disclosed to non-employees, shall be reviewed by a Company IP attorney prior to the disclosure, so that trade secrets and any other Company confidential information are not disclosed.

10. Employee Training

Employees and contractors shall receive IP training as a part of Company's New Hire Orientation, as applicable. The IP training portion shall include the topics of trade secrets and Company's trade secret policy. Thereafter, employees and contractors shall have periodic certifications and policy acknowledgements of IP and Trade Secret Policy training.

11. Off-Boarding Process

Exit interviews shall be conducted for all employees and contractors who have been terminated or are otherwise departing Company. During the exit interview, at least the following steps will be performed:

- a. Upon resignation or termination, Company IT shall be alerted, and the departing employee or contractor shall have their e-mail access and network access disabled. All employee or contractor passwords shall be terminated. Any laptops, phones, or other company provided devices will be retrieved by IT, and employee or contractor shall sign an acknowledgment that all company-provided laptops, documents, etc. have been returned.
- b. The employee or contractor shall be provided with a copy of the agreements from Section 2 herein, including the Confidentiality Agreement which references the employee's or contractor's continuing duty to keep trade secrets (and other Company confidential information) confidential. The employee or contractor will be reminded of their continuing duty with respect to Company confidential information and trade secrets and shall sign an acknowledgement of such reminder.
- c. Access keys, keys to desks or cabinets, company credit card, and/or key cards shall be returned to Building Security and/or Human Resources (HR).
- d. Any laboratory or engineering notebooks shall be retrieved and inventoried by the Company IP department. The Company IP attorney shall remove the employee from any authorization lists.
- e. If a personal device was used for work related duties, it shall be cleansed of any sensitive company information.

- f. Request IT to monitor any downloads of Company information via portable devices by departing employee and/or e-mails to employee personal e-mail or out of Company network account.

An Exit Interview Form (to be completed prior to employee or contractor departure) should be used as part of the off-boarding process. For additional information, please consult the *Employee Handbook* and/or Human Resources (HR).

12. Remedies for Trade Secret Misappropriation

Trade secret misappropriation is governed by State (or in Canada Provincial) and Federal laws. Remedies for trade secret misappropriation may include injunctive relief, monetary damages, attorneys' fees, litigation costs, and in some cases, criminal sanctions including fines and imprisonment.

13. Whistleblower Immunity Notice under the Defend Trade Secrets Act of 2016

An employee or contractor will be immune from an action that would otherwise count as trade secret misappropriation if the disclosure is made (i) in confidence to a Federal, State, or local government official, either directly or indirectly, or to an attorney; and (ii) solely for the purpose of reporting or investigating a suspected violation of law; or is made in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal. (18 U.S.C. 1833(b)).

This notice shall be included in Confidentiality or Non-Disclosure Agreements and NDAs entered by Company described in Section 2 herein.

Related Policies:

Employee Handbook

Clean Desk Policy

Bring Your Own Device (BYOD)

Global Marking Policy – Confidential Information

営業秘密方針

範囲

このポリシーは、企業が所有する、企業秘密として識別される、情報を保護するための、企業の全従業員（従業員は、パートタイムとフルタイム、一時的および永続的を指す）及び請負業者に当てはまる、手順と対策を定める。

ポリシー

1. 営業秘密の定義

営業秘密とは、秘密にされており、その秘密としての地位のために、経済的価値又は競争上の優位性を、企業に与える情報である。営業秘密と見なすことができる情報の例には、方式、パターン、アルゴリズム、編集、プログラム、方法、技術、顧客リスト、データセット又は編集、製品ロードマップ、価格設定スケジュール、失敗した実験、製造方法などが含まれるが、これらに限定されない。

営業秘密に該当する情報は、企業の知的財産（IP）委員会によって、そのように特定され、営業秘密へのアクセスを許可された従業員は、その秘密性を維持する責任を負う。

情報を営業秘密又は企業の機密情報と見なすか、あるいは、他の形式の IP で保護するかを検討する際の要素は、次のとおりである。

- 1) 情報がビジネス外で知られている範囲
- 2) 情報がビジネス内で知られている範囲
- 3) 情報の秘密を守るために使用される措置の範囲
- 4) リバースエンジニアリングの容易さ又は難しさ
- 5) 企業や競合他社にとっての情報の価値
- 6) 情報を開発するための努力/コスト

特定の法管轄域では、営業秘密を、ビジネスで継続的に使用する必要がある。

2. 入社時の確認および雇用契約

- a. 入社手続のある時点で、従業員又は請負業者は、第三者に属する営業秘密、発明、その他の所有情報及び機密情報を、使用又は開示しないことを確認する。第三者の営業秘密および所有情報に関する確認書が提出される。
- b. 雇用主/従業員又は雇用主/請負業者の関係が始まる前、若しくは、意味のある変更（昇進や配属の変更など）の前、および何らかの営業秘密が開示される前に、従業員又は請負業者は、少なくとも以下を含む契約に署名する必要がある。

- i. IP 譲渡：すべての従業員又は請負業者は、IP 譲渡に署名する必要がある。契約には、従業員が、明示的に、雇用中、及び、雇用に関連して開発した、営業秘密を含む IP を、所有者として企業に譲渡する現在の譲渡が含まれる。同様の譲渡は、該当する場合は、コンサルタント、ライセンシー、又は他の第三者によっても署名されるものとする。
- ii. 機密保持義務条項：すべての従業員または請負業者は、企業の情報及び営業秘密に関する機密保持義務を認める契約に署名する。同様の契約は、コンサルタント、ライセンシー、又は他の第三者によっても署名されるものとする。
- iii. 非競争/非勧誘：法律で許されている範囲で、契約には、従業員又は請負業者が、競合他社との間で雇用受入れ、又はサービス提供、企業との競争、若しくは、元雇用主の顧客または従業員の勧誘を、禁止する条項が含まれる。

詳細は、就業規則及び/又は人事課にて、参照すること。

3. 第三者との契約

第三者と契約関係を結ぶ前に、企業の機密情報（特に営業秘密情報）を共有するより先に、機密保持契約（NDA）または機密保持条項を含む契約を締結しなければならない。営業秘密を第三者と共有する場合は、法務部に警告し、追加の保護を与えるため、NDA 中の追加の契約条項、又は、その他の契約を含めることができるようする。

4. 物理的な安全性措置

- a. 施設のセキュリティ対策：施設への出入りは、写真付き ID が必要な訪問者のサインイン記録、訪問者の機密保持契約（NDA）、すべての訪問者の事前承認、及び、監視カメラにより、管理並びに監視されなければならない。すべての訪問者は、現場付添いを要するものとし、記録機能を備えたデバイス（カメラ、ビデオカメラ、ストップウォッチ、またはこれらの機能を備えたスマートフォンなど）を現場で使用することは禁じられている。
- b. アクセスの制限：建物へのアクセスは、許可された従業員と請負業者にのみ発行される、バッジを必要とする、施錠されたドアによって制限される。営業秘密のすべての物理的実施形態は、プロトタイプ、開発中モデル、又は、実際に使用されている実施例かにかかわらず、施錠され、視界に入らない、制限領域に維持されるものとする。従業員又は請負業者は、使用していないときは、営業秘密を含む作業資料又はファイルを、施錠された机またはファイリングキャビネットに入なければならない（整頓された机ポリシーを参照）。

5. マーキング

営業秘密は、当社のグローバルマーキングポリシーに従って、厳重に機密として目立つようにマークされる。このマーキングは、営業秘密情報を、他の企業の機密情報と区別する。したがって、営業秘密情報の場合、すべての物理的文書およびデジタルファイルには、ヘッダー、フッター、または、透かしのいずれかの形式で「社内厳重機密」を含める必要がある。営業秘密情報を、コピー又はダウンロードできる場合は、そのような文書又はデジタルファイルのコピーは、常に追跡、監視され、使用後に破棄される。

6. 営業秘密の保管

- a. 営業秘密の特定と説明：情報が営業秘密として特定されると、企業の知的財産弁護士が営業秘密の簡単な説明を作成する。
- b. 保護措置：営業秘密は、企業の機密情報より厳重な方法で、維持および保護される。すべての営業秘密は、パスワードで保護された、企業が管理するネットワーク上の営業秘密データベースに保存され、パスワードは、被許可者（第7条で定義）のみが知っているものとする。必要に応じて、追加の暗号化手段を使用できる。データベースは、アクセスが許可されている、企業の IP 弁護士及び/または情報技術（IT）課によって、保持される。営業秘密は、他の企業の機密情報から分離され、企業が管理するネットワークを介してのみアクセス可能で、企業の内部プライベートネットワーク（VPN）を介する場合を除き、他のネットワーク、クラウドストレージ、またはインターネットを介してアクセスすることはできない。営業秘密情報を含むラップトップやハードドライブなどの古いハードウェアは、廃棄、リサイクルするのではなく、物理的に破壊する必要がある。

7. 限られた、知る必要のあるアクセス

- a. **責任ある従業員**：企業の米国 IP 弁護士又は IP 委員会によって指定された従業員は、このポリシーの要件が、その営業秘密について満たされていることを確認することで、各営業秘密の秘密性を維持する責任を負う。
- b. **被許可者に限定**：許可された者による営業秘密へのアクセス又は使用は、その者が職務を遂行するために、営業秘密にアクセス又は使用する必要がある場合にのみ許可される。許可された者は、必要な場合に限り、営業秘密又は営業秘密の一部をコピーし、職務を遂行することができる。そのようなコピーはすべて、必要がなくなると、すぐに破棄、即ち、解読、再構築できないようにされる。
- c. 訪問者は、訪問中に閲覧又はアクセスされた情報の開示、並びに、記録装置（カメラ、携帯電話、USB ドライブなど）の制限区域内持込みが、いずれも禁止され、企業機密情報にアクセスする可能性のある場所では、従業員の同伴を要する旨を確認する書面に署名する必要がある。
- d. **電子情報管理**：
 - i. 営業秘密へのアクセスは、許可された人物のみ、かつ、許可された手段のみを介するよう、制限される。

- ii. 営業秘密に関連する情報が許可された者の間で共有する必要がある場合、それは安全な転送手段、つまり暗号化された電子メール又は安全なファイル転送を介して行われる。
- iii. 営業秘密へのアクセスを許可された者のリストは、各営業秘密の責任ある従業員及び/又は企業の IP 弁護士によって維持される。

8. 保護されたネットワーク及び携帯

- a. **ネットワークとデバイスのセキュリティ**：ネットワークとデバイスのセキュリティソリューションは、通常の業務と同様に、企業の IT 部門によって維持される。
- b. **個人用デバイス**：従業員と請負業者は、企業の個人所有デバイス持参（BYOD）ポリシーに準拠していない限り、仕事関連の問題での個人用デバイス使用を禁止している、企業のデバイス使用に関するポリシーに従う。これにより、雇用主と請負業者は、営業秘密情報を、個人のデバイス上にダウンロード、又は、それを使用することが、禁止される。
- c. **ポータブルデバイスまたはドライブ**：企業のコンピューターでのポータブルデバイス又はドライブの使用は許可されない。

9. 所有データ管理

公に開示される、又は、その他非従業員に開示される、すべてのプレゼンテーション、記事、及び研究論文は、営業秘密及びその他企業の機密情報が開示されないように、開示前に、企業の IP 弁護士によってレビューされる。

10. 従業員研修

従業員と請負業者は、必要に応じて、企業の新入社員オリエンテーションの一環として、IP トレーニングを受ける。IP トレーニングの部分には、営業秘密および企業の営業秘密ポリシーのトピックが含まれる。その後も、従業員と請負業者は、IP および営業秘密ポリシートレーニングの定期的な認証とポリシー確認を得る必要がある。

11. 退職時手順

退職面接は、解雇された、又は、企業を辞めた全従業員及び請負業者に対して、実施される。終了時面接では、少なくとも次の手順が実行される。

- a. 辞任または退職すると、企業の IT に警告が発せられ、退職した従業員または請負業者の、電子メールアクセスとネットワークアクセスを無効にする必要がある。すべての従業員又は請負業者のパスワードは終了する。ラップトップ、電話、その他の企業が提供するデバイスは、IT によって取り返され、従業員又は請負業者は、企業が提供するすべてのラップトップ、ドキュメントなどが、返却されたことの確認書に署名する必要がある。
- b. 従業員または請負業者には、従業員または請負業者の、営業秘密（およびその他の企業の機密情報）の機密性を保持する継続的な義務に言及する、機密保持契約

を含む、本契約第 2 条以降のコピーが提供される。従業員または請負業者は、企業の機密情報および営業秘密に関する、継続的な義務について注意喚起され、その確認書に署名する。

- c. アクセスキー、デスクまたはキャビネットへのキー、企業のクレジットカード、および/またはキーカードは、施設セキュリティ課および/又は人事課（HR）に返却する。
- d. 実験室ノートブックまたはエンジニアリングノートブックは、企業の IP 部門が取得して、インベントリを作成する必要がある。企業の IP 弁護士は、許可リストから従業員を削除する。
- e. 個人のデバイスが仕事関連の職務に使用された場合は、企業の機密性ある情報をすべて削除しなければならない。
- f. 退職する従業員による、ポータブルデバイスを介した、及び/又は、企業のネットワークアカウントから従業員の個人的な電子メール宛電子メールの送信による、企業情報のダウンロードを監視するよう IT に要求する。

退職手続の一環として、終了面接フォーム（従業員又は請負業者の出発前に記入する必要がある）を使用する必要がある。詳細は、従業員ハンドブック及び/又は人事課（HR）にて参照すること。

12. 営業秘密侵害への救済

営業秘密の侵害は、州法（またはカナダ州法）及び連邦法が適用になる。営業秘密の侵害に対する救済には、差止めによる救済、金銭的損害賠償、弁護士費用、訴訟費用、場合によっては、罰金や懲役などの刑事制裁が含まれる場合がある。

13. 2016 年営業秘密保護法による内部告発者免責

もし、開示が (i) 直接あるいは間接に、連邦、州、又は地方政府公務員に、又は、弁護士に、内密になされている、(ii) 法律違反の疑いを報告または調査することのみを目的としている場合、または、訴訟その他の手続きで提出された、訴状又はその他の文書で行われ、そのような提出が封印されている場合は、従業員または請負業者は、営業秘密の侵害と見なされる行為から免責される。(18 U.S.C. 1833(b))

この通知は、本第 2 条に記載されている、企業が締結した、機密保持または非開示契約、及び NDA に、含まれる。

関連トピック:

就業規則

整頓された机ポリシー

個人所有デバイス持参 (BYOD) ポリシー

グローバルマーケティングポリシー - 機密情報

Confidentiality and Proprietary Rights Agreement (CA)

This Employee Confidentiality and Proprietary Rights Agreement ("**Agreement**") is entered into by and between [], a California [], (the "**Employer**") and [] (the "**Employee**") (the Employer and the Employee are collectively referred to herein as the "**Parties**") as of [], 2021 (the "**Effective Date**").

In consideration of the Employee's employment by the Employer, which the Employee acknowledges to be good and valuable consideration for her obligations hereunder, the Employer and the Employee hereby agree as follows:

1. Confidentiality and Security.

(a) Confidential Information. The Employee understands and acknowledges that during the course of employment by the Employer, she will have access to and learn about confidential, secret and proprietary documents, materials, data, and other information, in tangible and intangible form, of and relating to the Employer and its businesses and existing and prospective customers, suppliers, investors and other associated third parties ("**Confidential Information**"). The Employee further understands and acknowledges that this Confidential Information and the Employer's ability to reserve it for the exclusive knowledge and use of the Employer is of great competitive importance and commercial value to the Employer, and that improper use or disclosure of the Confidential Information by the Employee might cause the Employer to incur financial costs, loss of business advantage, liability under confidentiality agreements with third parties, civil damages and criminal penalties.

For purposes of this Agreement, Confidential Information includes, but is not limited to, all information not generally known to the public, in spoken, printed, electronic or any other form or medium, relating to: business processes, practices, research, operations, services, strategies, techniques, contracts, negotiations, know-how, trade secrets, work-in-process, databases, accounting records, legal information, marketing information, and customer lists of the Employer or its businesses or any existing or prospective customer, supplier, investor or other associated third party, or of any other person or entity that has entrusted information to the Employer in confidence.

The Employee understands that the above list is not exhaustive, and that Confidential Information also includes other information that is marked or otherwise identified as confidential or proprietary, or that would otherwise appear to a reasonable person to be confidential or proprietary in the context and circumstances in which the information is known or used.

The Employee understands and agrees that Confidential Information developed by her in the course of her employment by the Employer shall be subject to the terms and conditions of this Agreement as if the Employer furnished the same Confidential Information to the Employee in the first instance. Confidential Information shall not include information that is generally available to and known by the public at the

time of disclosure to the Employee, provided that such disclosure is through no direct or indirect fault of the Employee or person(s) acting on the Employee's behalf.

(b) Disclosure and Use Restrictions. The Employee agrees and covenants:

(i) Employee covenants:

(A) to treat all Confidential Information as strictly confidential;

(B) not to directly or indirectly disclose, publish, communicate, or make available Confidential Information, or allow it to be disclosed, published, communicated or made available, in whole or part, to any third party not having a need to know and authority to know and to use the Confidential Information in connection with the business of the Employer and, in any event, not to anyone outside of the direct employ of the Employer, except as required in the performance of any of the Employee's authorized employment duties to the Employer or with the prior consent of an authorized officer acting on behalf of the Employer in each instance (and then, such disclosure shall be made only within the limits and to the extent of such duties or consent); and

(C) not to access or use any Confidential Information, and not to copy any documents, records, files, media, or other resources containing any Confidential Information, or remove any such documents, records, files, media or other resources from the premises or control of the Employer, except as required in the performance of any of the Employee's authorized employment duties to the Employer or with the prior consent of an authorized officer acting on behalf of the Employer in each instance (and then, such access and use shall only be within the limits and to the extent of such duties or consent). The Employee understands and acknowledges that the Employee's obligations under this Agreement regarding any particular Confidential Information begin immediately and shall continue during and after the Employee's employment by the Employer until the Confidential Information has become public knowledge other than as a result of the Employee's breach of this Agreement or a breach by those acting in concert with the Employee or on the Employee's behalf.

(ii) Permitted disclosures. Nothing in this Agreement shall be construed to prevent disclosure of Confidential Information as may be required by applicable law or regulation, or pursuant to the valid order of a court of competent jurisdiction or an authorized government agency, provided that the disclosure does not exceed the extent of disclosure required by such law, regulation, or order. The Employee shall promptly provide written notice of any such order to an authorized officer of the Employer.

(iii) Nothing in this Agreement prohibits or restricts the Employee (or Employee's attorney) from initiating communications directly with, responding to an inquiry from, or providing testimony before the Securities and Exchange Commission (SEC), the Financial Industry Regulatory Authority (FINRA), any other self-regulatory organization, or any other federal or state regulatory authority regarding a possible securities law violation.

(iv) Nothing in this Agreement in any way prohibits or is intended to restrict or impede the Employee from discussing the terms and conditions of her employment with co-workers or union representatives, exercising her rights under Section 7 of the National Labor Relations Act, exercising protected rights to the extent that such rights cannot be waived by agreement, or otherwise disclosing information as permitted by law.

(v) Notice of Immunity Under the Economic Espionage Act of 1996, as amended by the Defend Trade Secrets Act of 2016. Notwithstanding any other provision of this Agreement:

(A) This Employee will not be held criminally or civilly liable under any federal or state trade secret law for any disclosure of a trade secret that is made: (1) in confidence to a federal, state, or local government official, either directly or indirectly, or to an attorney and solely for the purpose of reporting or investigating a suspected violation of law; or (2) in a complaint or other document that is filed under seal in a lawsuit or other proceeding.

(B) If the Employee files a lawsuit for retaliation by the Employer for reporting a suspected violation of law, the Employee may disclose the Employer's trade secrets to the Employee's attorney and use the trade secret information in the court proceeding if the Employee (1) files any document containing the trade secret under seal; and (2) does not disclose the trade secret, except pursuant to court order.

(vi) Duration of Confidentiality Obligations. The Employee understands and acknowledges that her obligations under this Agreement with regard to any particular Confidential Information shall commence immediately upon the Employee first having access to such Confidential Information (whether before or after she begins employment by the Employer) and shall continue during and after her employment by the Employer until such time as such Confidential Information has become public knowledge other than as a result of the Employee's breach of this Agreement or breach by those acting in concert with the Employee or on the Employee's behalf.

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the Effective Date above.

機密保持義務契約

この従業員の機密保持義務（「本契約」）は、カリフォルニア州の[]である[]（「雇用主」）と[]（「従業員」）（雇用者と従業員を総称して「当事者」と言う。）との間で2021年 月 日（「発効日」）に締結される。

雇用主による従業員の雇用を考慮し、従業員は、本契約に基づく義務に対する、十分かつ価値のある対価と認め、雇用主と従業員は、以下のとおり合意する。

1. 機密性と安全性.

(a) 機密情報。従業員は、雇用主による雇用の過程で、雇用主、その事業、既存および将来の顧客、サプライヤー、投資家、その他の関連する第三者に関連する、有形及び無形の機密、秘密、及び所有される、文書、資料、データ、その他の情報（「機密情報」）にアクセスし、それを知ることがあることを、理解し、確認する。従業員はさらに、この機密情報、及び、雇用主が、独占的な知識と使用のために、それを留保することができる能力が、雇用主の競争上非常に重要で、商業的価値があること、並びに、従業員は、従業員による機密情報の不正使用又は開示が、金銭的費用、ビジネス上の優位性の喪失、第三者との機密保持契約に基づく責任、民事上の損害賠償、及び刑事罰を、雇用主に負わせる可能性があることを理解し、確認する。

本契約の目的上、機密情報には、雇用主とその事業、既存又は将来の顧客、サプライヤー、投資家、その他の関連する第三者、若しくは、情報を雇用主に秘密裏に委託したその他の個人又は団体についての、ビジネスプロセス、慣行、調査、運用、サービス、戦略、技術、契約、交渉、ノウハウ、営業秘密、開発品、データベース、会計記録、法的情報、マーケティング情報、顧客リストに関する、一般に知られていない、口頭、印字、電子、その他の形式又は媒体中の、全情報を含み、これに限られない。

従業員は、上記のリストが網羅的ではなく、機密情報には、機密又は所有された情報、としてマーク、あるいは他の方法で識別された情報、若しくは、情報が知られた、又は、使用された文脈や状況で、合理的な者にとり、機密情報又は所有情報と考えられる、その他の情報も含まれることを理解する。

従業員は、雇用主による雇用の過程で、自身が作成した機密情報は、雇用主が、同じ機密情報を従業員に提供したかのように扱われ、本契約の条件に従うべきことを理解し、同意する。機密情報には、従業員又は従業員に代わって行動する人物の、直接的又は間接的な過失によるものでない限り、従業員への開示時に、一般に利用可能か、一般に知られている情報は含まれない。

(b) 開示と使用の制約。従業員は、以下に同意し、合意する：

(i) 従業員は、下記のように、誓約する：

(A) 全機密情報を厳に機密として扱う；

(B) 機密情報を、直接的又は間接的に開示、公開、伝達、又は、利用可能にしない、知る必要がなく、知る権限を持たない第三者に、その全部又は一部を開示、公開、伝達、又は、利用可能にしない、雇用主の事業に関連して、機密情報を使用する、いかなる場合でも、雇用主に対する、従業員の許可された職務の履行に必要な場合、又は、雇用主を代理する権限のある役員の事前の同意を得た場合以外、雇用主から直接に雇用された者以外には開示しない（以後、開示は、そのような義務又は同意の範囲内でのみ行われる）；

(C) 雇用主に対する、従業員の許可された職務の履行に必要な場合、又は、雇用主を代理する権限のある役員の事前の同意を得た場合以外、機密情報にアクセス又は使用したり、機密情報を含む文書、記録、ファイル、メディア、その他の資料をコピーしたり、そのような文書、記録、ファイル、メディア、その他の資料を雇用主の施設又は管理から持ち出したりしない。（以後、アクセスと使用は、そのような義務又は同意の範囲内でのみ行われる）。従業員は、特定の機密情報に関する本契約に基づく従業員の義務は、直ちに施行され、雇用主による従業員の雇用中および雇用後も、従業員による、あるいは、従業員と協力して、又は従業員に代わって行動する者による、機密保持義務の違反の結果として以外に、機密情報が公に知られるようになるまで、継続することを理解し、確認する。

(ii) 許可される開示。本契約のいかなる条項も、適用される法律又は規制によって、若しくは、管轄裁判所又は政府機関の有効な命令に従って要求される場合、開示が、それら法律、規制、又は命令によって要求される開示の範囲を超えない限り、機密情報の開示を妨げるとは解釈されない。従業員は、雇用主を代表する権限のある役員に、そのような命令についての書面による通知を、迅速に提供する。

(iii) 本契約のいかなる条項も、従業員（又は従業員の弁護士）が、証券取引法違反の可能性に関して、証券取引委員会（SEC）、金融業界規制当局（FINRA）、その他の自主規制機関、その他の連邦又は州の規制当局と、直接に会話を開始したり、問い合わせに応答したり、証言を提供したりすることを禁止又は制限するものではない。

(iv) 本契約のいかなる条項も、従業員が、同僚又は組合の代表者と、雇用条件について話し合い、全国労働関係法第7条に基づく権利を行使し、保護された権利を、そのような権利が合意によって放棄できない範囲で行使し、又は、法律が許可するように情報を開示することを、禁止するものでなく、制限又は妨害することを意図しない。

(v) 2016年連邦営業秘密保護法によって改正された、1996年経済スパイ活動法に基づく、免責の通知。

本契約の他の規定にもかかわらず

(A) 従業員は、次のような営業秘密の開示について、連邦又は州の営業秘密法に基づいて、刑事上又は民事上の責任を負わない：(1) 直接又は間接に、連邦、州又は地方政府の公務員に対し、若しくは、弁護士を介して、内密に、法律違反の疑いを報告、又は、調査することのみを目的とする場合、又は、(2) 訴訟又はその他の手続きで、封印されて提出された訴状又はその他の文書中の場合。

(B) 従業員が法律違反の疑いを報告したとして、雇用主による報復訴訟が提起された場合、従業員が(1) 営業秘密を含む文書を封印下に提出し；(2) 裁判所の命令に基づく場合を除き、営業秘密を開示しない場合には、従業員は、雇用主の営業秘密を従業員の弁護士に開示し、裁判所の手続きで企業の秘密情報を使用することができる。

(vi) 機密保持義務の期間。従業員は、特定の機密情報に関する本契約に基づく義務は、従業員がそのような機密情報に最初にアクセスした時点で直ちに開始し（雇用主による雇用を開始する前か後かにかかわらず）、雇用主による雇用の間、及び、その後も、従業員による、若しくは、従業員と協力している、又は、従業員に代わって行動する者による、本契約の違反以外の結果、そのような機密情報が公に知られるようになるまで、継続することを理解し、確認する。

本契約の証として、当事者は、発効日に、本契約を署名捺印した。

3 退職後の競業避止契約書の例

NON-COMPETITION AGREEMENT

SECTION 1. Definition.

(a) Competitive Business means any corporation, partnership, association, or other person or entity, including but not limited to Executive, (i) which competes directly, or is planning to compete directly, with the Company with respect to the design, development, manufacture, remanufacture, assembly, marketing, sales, or service of [], or any other business of the Company, that was related to Executive's work, practice, customer relationship, planning, operation, marketing, purchasing, or sales responsibility, or that Executive received any Confidential Information or Trade Secrets about, at any time within eighteen (18) months prior to termination of Executive's employment with the Company or any of its subsidiaries, and (ii) which engages or plans to engage in such competition in the demographic regions that the Company sold or distributed, or actively attempts to sell or distribute, such products or services within eighteen (18) months prior to termination of Executive's employment with the Company or any of its subsidiaries.

(b) Confidential Information shall mean information, not generally known in the trade or industry, which Executive learns or creates during the course of Executive's employment with the Company or any of its subsidiaries, which may include but is not limited to product specifications, manufacturing procedures, methods, equipment, compositions, data compilations, technologies, formulas, know-hows, research and development programs, sales methods, customer lists, customer information, computer programs and other confidential technical or business information and data. Confidential Information shall not include any information that (A) is or becomes generally available to the public other than as a result of a disclosure by Executive in violation of this Non-Competition Agreement or (B) becomes available to Executive on a non-confidential basis from a source other than the Company or its affiliates which is not prohibited from disclosing such information to Executive by a legal, contractual or fiduciary obligation to the Company or any other person.

(c) Trade Secret(s) means information, including a formula, pattern, compilation, program, device, method, technique or process, that derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons in the same business circle or industry, and that is the subject of efforts to maintain its secrecy that are reasonable under the circumstances.

SECTION 2. Non-Competition; Non-Solicitation.

(a) Noncompetition. During the term of Executive's employment with the Company or any of its subsidiaries and for eighteen (18) months following the termination of such employment for any reason, Executive shall not, directly or indirectly, participate in, consult with, be employed by, or assist with the organization, planning, ownership, financing, management, operation or control of any Competitive Business in any capacity in which, in the absence of this Agreement, Confidential Information, Trade Secrets or goodwill of the Company would reasonably be considered useful.

(b) Nonsolicitation. During the term of Executive's employment with the Company or any of its subsidiaries and for eighteen (18) months following the termination of such employment for any reason, Executive shall not, directly or indirectly, on behalf of any Competitive Business, either by himself or by providing substantial assistance to others, solicit to terminate employment with the Company or any of its subsidiaries, or to accept or begin employment with or service to any Competitive Business, any employee of the Company whom Executive supervised or about whom Executive gained Confidential Information at any time during the last eighteen (18) months of Executive's employment with the Company or any of its subsidiaries.

SECTION 3. No Right to Continued Employment.

Nothing in this Non-Competition Agreement shall confer upon Executive any right to continue in the employ of the Company or shall interfere with or restrict in any way the rights of the Company, which are hereby reserved, to discharge Executive at any time for any reason whatsoever, with or without cause.

SECTION 4. No Conflicting Agreements.

Executive warrants that Executive is not bound by the terms of a confidentiality agreement, non-competition or other agreement with a third party that would conflict with Executive's obligations hereunder.

SECTION 5. Remedies.

(a) In the event of breach or threatened breach by Executive of any provision hereof, the Company shall be entitled to seek temporary or preliminary injunctive relief or other equitable relief to which either of them may be entitled, without the posting of any bond or other security.

(b) The period of time during which the restrictions set forth in Section 2(a) hereof will be in effect will be extended by the length of time during which Executive is in breach of the terms of those provisions as finally determined by an arbitrator or any court of competent jurisdiction.

SECTION 6. Successors and Assigns.

This Non-Competition Agreement shall be binding upon Executive and Executive's heirs, assigns and representatives and inure to the benefit of the Company and its successors and assigns, including without limitation any entity to which substantially all of the assets or the business of either of the Company are sold or transferred. The obligations of Executive are personal to Executive and shall not be assigned by Executive.

SECTION 7. Severability.

It is expressly agreed that if any restrictions set forth in this Non-Competition Agreement are found by any court having jurisdiction to be unreasonable because they are too broad in any respect, then and in each such case, the remaining provisions herein contained shall, to the greatest extent permitted under applicable law, nevertheless, remain effective, and this Non-Competition Agreement, or any portion hereof, shall, to the extent permitted by applicable law, be considered to be amended, so as to be

considered reasonable and enforceable by such court, and the court shall specifically have the right to restrict the time period or the business or geographical scope of such restrictions to any portion of the time period, business or geographic areas to the extent the court deems such restriction to be necessary to cause the covenants to be enforceable and, in such event, the covenants shall be enforced to the extent so permitted and the remaining provisions shall be unaffected thereby. In such event, the parties hereto agree to execute all documents necessary to evidence such amendment so as to eliminate or modify any such unreasonable provision in order to carry out the intent of this Non-Competition Agreement insofar as possible and to render this Non-Competition Agreement enforceable in all respects as so modified. The covenants contained in this Section 7 shall be construed to extend to separate jurisdictions or sub-jurisdictions of the United States in which the Company, during the term of Executive's employment, have been or are engaged in business, and to the extent that any such covenant shall be illegal and/or unenforceable with respect to any jurisdiction, said covenant shall not be affected thereby with respect to each other jurisdiction, such covenants with respect to each jurisdiction being construed as severable and independent. The restrictive covenant provisions of this Non-Competition Agreement shall govern to the extent there is any conflict between their terms and the terms of any other agreement or understanding with the Company.

競業禁止合意

第 1 条. 定義.

(a) 競合ビジネスとは、貴殿を含むが限定されない、以下の条件を充たす、企業、組合、協会、その他の個人又は団体を意味する。(i) []の製造、再製造、組立て、マーケティング、販売、又はサービスに関して、若しくは、(1)貴殿の仕事、慣行、顧客関係、計画、運用、マーケティング、購入、又は販売の責任に関連した、又は、(2)貴殿が、当社またはその子会社との雇用が終了する前の 18 か月以内のいずれかの時点で、関連した機密情報または営業秘密を受け取った、当社の他の事業に関して、直接に当社と競合する、又は、競合する予定である、(ii) 貴殿の当社又はその子会社との雇用が終了する前の 18 か月以内に、当社が、そのような製品またはサービスを販売または配布した、若しくは、積極的に販売または配布を試みた地域において、当社と競争する、あるいは、競争を予定する。

(b) 機密情報とは、当社またはその子会社と貴殿間の雇用の過程で、貴殿が知る、又は、作成する、取引界、業界で一般的に知られていない情報を意味する。これには、製品の仕様、製造手順、方法、機器、構成、データ編集、技術、方式、ノウハウ、研究開発プログラム、販売方法、顧客リスト、顧客情報、コンピュータープログラム、その他の機密の技術情報又はビジネス情報及びデータが含まれるが、これらに限定されない。機密情報には、

(A) この競業禁止合意に違反する貴殿による開示による結果を除いて、一般に利用可能である、又は、一般に利用可能となる情報、若しくは、(B) 当社その他の者に対する法的、契約上、又は受託者責任により、貴殿への情報開示が禁止されない、当社またはその関連会社以外の情報源から、内密でない状況で、貴殿に利用可能となった情報は、含まれない。

(c) 営業秘密とは、方式、パターン、編集、プログラム、デバイス、方法、技術、またはプロセスを含む情報を意味し、一般に知られていないこと、及び、同じ業界または産業の他者により、適正な方法で容易に確認できないことから、現実の、又は、潜在的な独立した経済的価値を導き出し、その状況下で、秘密性を維持するための合理的な努力の対象となっている。

第 2 条. 競業禁止； 勧誘禁止.

(a) 競業禁止 当社又はその子会社と貴殿との雇用期間中、及び、いずれかの事由による雇用終了後 18 か月間、貴殿は、競合ビジネスの組織、計画、所有、資金調達、管理、運営または支配へ、本契約のない場合に、当社の機密情報、営業秘密、又は、当社ののれんが、それに合理的に有用と見なされうる地位において、直接的または間接的に、参加、諮問、就業又は支援をしない。

(b) 勧誘禁止 当社又はその子会社と貴殿との雇用期間中、及び、いずれかの事由による雇用終了後 18 か月間、貴殿は、直接的または間接的に、競合ビジネスに代

わって、自身で、あるいは、他者に相当な支援を提供することで、貴殿が当社又はその子会社との雇用から最終 18 か月間の任意の時点で、貴殿が監督した、又は、貴殿がその者に関する機密情報を入手した、当社の従業員に対し、当社又はその子会社との雇用の終了、若しくは、競合ビジネスとの間の雇用関係又はサービスの、受諾又は開始を唆してはならない。

第 3 条. 継続雇用の権利の不存在

この競業避止合意のいかなる条項も、当社との雇用を継続する権利を貴殿に付与するものではなく、また、理由の有無、如何を問わず、いつでも貴殿を解雇する当社の権利を、それは留保されているが、妨害または制限するものではない。

第 4 条. 矛盾する合意の不存在.

貴殿は、本契約に基づく貴殿の義務と矛盾する、機密保持契約、競業避止義務、又は、第三者とのその他の契約に、拘束されないことを保証する。

第 5 条. 救済.

(a) 本契約のいずれかの条項の貴殿による違反または違反の恐れがある場合、当社は、保証金その他の担保なく、いずれか享受することのできる、一時的又は暫定的差止命令その他の衡平法上の救済を受けることができる。

(b) 本契約の第 2 条 (a) に規定された制限が有効である期間は、仲裁人または管轄権を有する裁判所によって、最終的に決定された、これらの規定条項違反の期間によって延長される。

第 6 条. 承継と譲渡.

この競業避止契約は、貴殿及び貴殿の相続人、譲受人、代理人を拘束し、当社、その後継者、及び譲受人（当社の実質的に全資産又は事業が売却又は譲渡された会社が含まれるが、これに限定されない。）の利益のために、効力を生じる。貴殿の義務は、貴殿に個人的なものであり、貴殿によって移転されることはできない。

第 7 条. 分離可能性.

管轄権を有する裁判所によって、この競業避止契約に定められた制限が、いずれかの事由で、広範すぎるために不合理であると判断された場合、本合意に含まれる残りの条項は、それにかかわらず、適用される法令の下で認められる最大の限度で、引き続き有効であり、この競業避止合意またはその一部は、適用される法令によって認められる範囲で、裁判所が、合理的かつ執行可能であると考えられるように、修正されたと見なされ、かつ、裁判所が、当該制限の期間、事業、又は地理的な範囲を、当該制限が法的拘束力を有するために必要な程度で、期間、事業、又は地理的の範囲を限定する権利を、特に有するものとする。そのような場合、

本合意は、許可された範囲で法的に執行され、残りの条項は、そこで影響を受けないものとする。そのような場合、当事者は、この競業避止合意の目的を可能な限り実行し、本合意を全ての点で修正後に執行可能となるように、不合理な条項を削除又は変更する旨の、修正を証明するために必要な、全ての文書を署名することに同意する。この第7条に含まれる規定は、貴殿の雇用期間中に、当社が事業を行った、又は、行っている米国内の各別の管轄区域又は準管轄区域にまで及ぶものと解釈される。本合意の制約が、いずれかの管轄域で、違法及び/又は執行不能であるものとされた程度で、当該制約は、他の管轄域では影響を受けないものとし、各管轄域に関して、当該制約は、分離可能かつ独立であると解釈される。本競業避止契約の制約条項は、その条件と当社の他の契約または合意の条件との間で矛盾がある場合、優先して適用される。

4 取引先との秘密保持契約書の例

NON-DISCLOSURE AGREEMENT

This Non-Disclosure Agreement (“Agreement”) dated _____, 20__ (the “Effective Date”), between _____, a _____ corporation (“Party A”) with offices at _____ and _____, a _____ corporation located at _____ (“Party B”).

1. Background. Party A and Party B (the “parties”) intend to engage in discussions and negotiations concerning a possible transaction or business relationship between them. In the course of such discussions and negotiations and in the course of any such transaction or business relationship, it is anticipated that each party will disclose or deliver to the other party and to the other party’s directors, officers, employees, agents or advisors (including, without limitation, attorneys, accountants, consultants, bankers, financial advisors and members of advisory boards) (collectively, “Representatives”) certain of its trade secrets or confidential or proprietary information for the purposes of enabling the other party to evaluate the feasibility of such transaction or business relationship and to perform its obligations and exercise its rights under any such transaction or business relationship that is agreed to between the parties (the “Purposes”). The parties have entered into this Agreement in order to assure the confidentiality of such trade secrets and confidential or proprietary information in accordance with the terms of this Agreement. As used in this Agreement, the party disclosing Proprietary Information (as defined below) is referred to as the “Disclosing Party”; the party receiving such Proprietary Information is referred to as the “Recipient”.

2. Proprietary Information. As used in this Agreement, the term “Proprietary Information” shall mean all trade secrets or confidential or proprietary information designated as such in writing by the Disclosing Party, whether by letter or by the use of an appropriate proprietary stamp or legend, prior to or at the time any such trade secret or confidential or proprietary information is disclosed by the Disclosing Party to the Recipient. Notwithstanding the foregoing, information which is orally or visually disclosed to the Recipient by the Disclosing Party, or is disclosed in writing without an appropriate letter, proprietary stamp or legend, shall constitute Proprietary Information if it would be apparent to a reasonable person, familiar with the Disclosing Party’s business and the industry in which it operates, that such information is of a confidential or proprietary nature the maintenance of which is important to the Disclosing Party. In addition, the term “Proprietary Information” shall be deemed to include: (a) any notes, analyses, compilations, studies, interpretations, memoranda or other documents prepared by the Recipient or its Representatives which contain, reflect or are based upon, in whole or in part, any Proprietary Information furnished to the Recipient or its Representatives pursuant hereto; and (b) the existence or status of, and any information concerning, the discussions between the parties concerning the possible transaction or business relationship.

3. Use and Disclosure of Proprietary Information. The Recipient and its Representatives shall use the Proprietary Information of the Disclosing Party only for the Purposes and such Proprietary Information shall not be used for any other purpose without the prior written consent of the Disclosing Party. The Recipient and its Representatives shall hold in confidence, and shall not disclose any Proprietary Information of the Disclosing Party; provided, however, that (i) the Recipient may make any disclosure of such information to which the Disclosing Party gives its prior written consent; and (ii) any

of the Proprietary Information may be disclosed by the Recipient to its Representatives who need to know such information in connection with the Purposes and who are informed of the confidential nature of such information and of the terms of this Agreement. In any event, the Recipient shall be responsible for any breach of this Agreement by any of its Representatives, and agrees, at its sole expense, to take reasonable measures to restrain its Representatives from prohibited or unauthorized disclosure or use of the Proprietary Information, Notwithstanding anything contained in this Agreement to the contrary, this Agreement shall not prohibit the Recipient from disclosing Proprietary Information of the Disclosing Party to the extent required in order for the Recipient to comply with applicable laws and regulations, provided that the Recipient provides prior written notice of such required disclosure to the Disclosing Party and takes reasonable and lawful actions to avoid and/or minimize the extent of such disclosure.

4. Limitation on Obligations. The obligations of the Recipient specified in Section 3 above shall not apply, and the Recipient shall have no further obligations, with respect to any Proprietary Information to the extent that such Proprietary Information:

(a) is generally known to the public at the time of disclosure or becomes generally known without Recipient or its Representatives violating this Agreement;

(b) is in the Recipient's possession at the time of disclosure;

(c) becomes known to the Recipient through disclosure by sources other than the Disclosing Party without such sources violating any confidentiality obligations to the Disclosing Party; or

(d) is independently developed by the Recipient without reference to or reliance upon the Disclosing Party's Proprietary Information.

5. Ownership of Proprietary Information. The Recipient agrees that it shall not receive any right, title or interest in, or any license or right to use, the Disclosing Party's Proprietary Information or any patent, copyright, trade secret, trademark or other intellectual property rights therein, by implication or otherwise. Each of the parties hereto represents, warrants and covenants that the trade secrets which it discloses to the other party pursuant to this Agreement have not been stolen, appropriated, obtained or converted without authorization.

6. Return of Proprietary Information. The Recipient shall, upon the written request of the Disclosing Party, return to the Disclosing Party all Proprietary Information received by the Recipient or its Representatives from the Disclosing Party (and all copies and reproductions thereof). In addition, the Recipient shall destroy: (i) any notes, reports or other documents prepared by the Recipient which contain Proprietary Information of the Disclosing Party; and (ii) any Proprietary Information of the Disclosing Party (and all copies and reproductions thereof) which is in electronic form or cannot otherwise be returned to the Disclosing Party. Alternatively, upon written request of the Disclosing Party, the Recipient shall destroy all Proprietary Information received by the Recipient or its Representatives from the Disclosing Party (and all copies and reproduction thereof) and any notes, reports or other documents prepared by the Recipient which contain Proprietary Information of the Disclosing Party. Notwithstanding the return or destruction of the Proprietary Information, the Recipient and its

Representatives will continue to be bound by their obligations of confidentiality and other obligations hereunder.

7. Securities. Recipient represents that it is aware, and will advise its representatives who are informed of the matters that are the subject of this Agreement, of the restrictions imposed by the applicable federal and state securities laws on the purchase or sale of securities by any person who has received material, non-public information regarding a company with publicly traded securities, as well as the restrictions making it unlawful to communicate such information to any other person when it is reasonably foreseeable that such other person is likely to purchase or sell securities in reliance upon such information.

8. Non-Solicitation of Employees Covenant. Each party agrees that during the term of this Agreement and for the period of two (2) years after the termination of this Agreement, it will not, either directly or through others solicit or attempt to solicit any employee of the other party with whom such party came into contact with during the evaluation of a possible transaction between the parties to become an employee, consultant or independent contractor to or for itself or any of its affiliates; provided, - however, that nothing contained herein shall be deemed to prohibit any party, either directly or through others, from (i) conducting any general solicitation not specifically targeted at any such employee, and, for the avoidance of doubt, the hiring or engagement by a party of any employee of the other party who responds to such general advertising or who approaches such party or any of its affiliates without any solicitation or inducement to leave the employ of the other party or any of its affiliates shall not be deemed a breach of this Section 8, or (ii) soliciting for employment or hiring any employee of the other party or any of its affiliates who was terminated by the other party or any of its affiliates; each subject to such employee's restrictive covenants

9. Miscellaneous.

(a) This Agreement supersedes all prior agreements, written or oral, between the parties relating to the subject matter of this Agreement. This Agreement may not be modified, changed or discharged, in whole or in part, except by an agreement in writing signed by the parties.

(b) This Agreement will be binding upon and inure to the benefit of the parties hereto and their respective heirs, successors and assigns.

(c) This Agreement shall be construed and interpreted in accordance with the internal laws of the Commonwealth of Massachusetts, without giving effect to the principles of conflicts of law thereof.

(d) The provisions of this Agreement are necessary for the protection of the business and goodwill of the parties and are considered by the parties to be reasonable for such purpose. The Recipient agrees that any breach of this Agreement will cause the Disclosing Party substantial and irreparable injury and, therefore, in the event of any such breach, in addition to other remedies which may be available, the Disclosing Party shall have the right to specific performance and other injunctive and equitable relief.

(e) The confidentiality obligations imposed by this Agreement shall continue with respect to a particular item of Proprietary Information until the fifth anniversary of the disclosure of such Proprietary Information to Recipient pursuant to this Agreement; provided, however, that the confidentiality

obligations imposed by this Agreement with respect to source code included in the Proprietary Information shall continue in perpetuity.

(f) For the convenience of the parties, this Agreement may be executed by facsimile and in counterparts, each of which shall be deemed to be an original, and both of which taken together, shall constitute one agreement binding on both parties.

EXECUTED as a sealed instrument as of the day and year first set forth above.

機密保持契約

_____で設立され、事業所を _____に置く、 _____
(“X”) と、 _____で設立され、事業所を _____に置く、
_____ (“Y”) は、20__ 年 _____日、 (「契約日」), 以下のとおり本機
密保持契約 (“本契約”) を締結した。

1. **背景** 当事者 X 及び当事者 Y (「当事者」) は、両者間の可能な取引又はビジネス関係に関する、議論及び交渉に従事することを意図する。そのような話し合いや交渉の過程、並びに、そのような取引や取引関係の過程で、各当事者は、相手方が、そのような取引又はビジネス関係の実現可能性を評価できるようにするため、及び、当事者間で合意されたそのような取引又はビジネス関係 (「目的」) の下で、その義務を履行し、その権利を行使するため、相手方及び相手方の取締役、役員、従業員、代理人、又は顧問 (、弁護士、会計士、コンサルタント、銀行家、財務顧問及び諮問委員会のメンバー) (総称して「代理人」) に、特定の営業秘密、機密情報、又は保有情報を、開示あるいは提供することを予定している。両当事者は、本契約の条項に従って、このような営業秘密、機密情報、又は保有情報の機密性を保証するために、本契約を締結した。本契約で、保有情報 (以下に定義) を開示する当事者は、「開示当事者」と呼ばれる。そのような保有情報を受け取る当事者は、「受領者」と呼ばれる。

2. **情報保有情報** 本契約で使用される、「保有情報」という用語は、そのような営業秘密、機密情報、又は保有情報が開示当事者から受領者に開示される時点、若しくは、それ以前に、開示当事者によって、書簡、適切な専有スタンプ、又は、説明文のいずれによるかを問わず、書面で指定された、すべての営業秘密、機密情報、又は保有情報を意味する。上記にかかわらず、開示当事者によって受領者に口頭又は視覚的に開示された情報、若しくは、適切な書簡、専有スタンプ、又は、説明文なく、書面で開示された情報は、開示当事者の事業及びその属する業界に通じた合理的な者に、当該情報が、機密、あるいは、保有される性質のもので、その維持が、開示当事者にとって重要であると明らかである場合、保有情報を構成する。さらに、「保有情報」という用語には、次のものが含まれると想定されている：(a) 本契約に従って受領者又はその代理人に提供される保有情報の、全体又は部分を含む、反映する、若しくは、基礎とする、受領者又はその代理人が用意した、ノート、解析、編集、調査、解釈、メモ、又は、他の書面、(b) 取引又はビジネス関係の可能性に関する、当事者間の話し合いの存在又は状況、及び、それらに関する情報。

3. **保有情報の使用及び開示** 受領者及びその代理人は、開示当事者の保有情報を本目的にのみ使用するものとし、かかる保有情報は、開示当事者の事前の書面による同意なしに、他の目的に使用できない。受領者とその代理人は、秘密性を保持し、開示当事者の保有情報を開示しない。ただし、(i) 受領者は、開示当事者が事前に書面で同意した情報を開示することができ、(ii) 保有情報のいずれかは、本目的に関連して、そのような情報を知る必要があり、当該情報の機密性、及び本契約の条項について知らされている代理人に、受領者によって開示される。いずれにせよ、受領者は、その代理人による本契約の違反に対して責任を負い、その代理人による、禁止される、又は、許可の無い、保有情報の開示、若しくは使用を制限するため、合理的な措置を自己の費用で講

じることと同意する。本契約中のこれに反する規定にもかかわらず、本契約は、受領者が、適用法及び規制を遵守するために必要な範囲で、事前に開示当事者に、必要な開示を書面で通知し、かつ、そのような開示を回避、及び/又は、範囲を最小化するために、適法な合理的行動を取ることを条件として、開示当事者の保有情報を開示することを禁じない。

4. 制限及び義務 下記に該当する保有情報に関しては、その限りで、前掲第3条で指定された受領者の義務が適用されず、受領者は、それ以上の義務を負わないものとする。

(a) 開示の時点で一般に知られている、若しくは、受領者又はその代理人が、本契約に違反することなく、一般に知られるようになる。

(b) 開示の時点で、受領者が所有している。

(c) 開示当事者以外の情報源からの開示で、受領者に知られるようになり、当該情報源が、開示当事者に対する秘密保持義務に違反していない。

(d) 開示当事者の所有情報を参照したり、依存したりすることなく、受領者が独自に開発した。

5. 保有情報の保有 受領者は、黙示的又はその他の方法により、開示当事者の保有情報、若しくは、その中の特許、著作権、営業秘密、商標、その他の知的財産権に対する権利、権原、利益、又は、ライセンスや使用权を、取得しないことに同意する。本契約の各当事者は、本契約に従って相手方当事者に開示する営業秘密が、許可なく盗取、侵害、取得、又は転換されていないことを、表明、保証、かつ、誓約する。

6. 保有情報の返却 受領者は、開示当事者の書面による要求に応じて、受領者又はその代理人が開示当事者から受け取った、すべての保有情報（及び、そのすべてのコピーと複製）を開示当事者に返却する。さらに、受領者は以下を破棄する：(i) 開示当事者の保有情報を含む、受領者が作成したメモ、レポート、又はその他の文書；(ii) 電子形式であるか、その他、開示当事者に返却することができない、開示当事者の保有情報（及び、そのすべてのコピーと複製）。あるいは、開示当事者の書面による要求に応じて、受領者は、受領者又はその代理人が開示当事者から受け取ったすべての保有情報（及び、そのすべてのコピーと複製）、並びに、開示当事者の保有情報を含む受領者が作成したメモ、レポート、又はその他の文書を、破棄する。保有情報の返却又は破棄にかかわらず、受領者及びその代理人は、引き続き、秘密保持義務、及び、本契約に基づくその他の義務に拘束される。

7. 証券 受領者は、適用される連邦及び州の証券法により、上場証券を保有する会社に関する重要な非公開情報を受領した者に、証券の購入又は売却について課された制限、並びに、当該情報を受領すると、それに依り、証券の購入又は売却することが、合理的に予測できる他人に、そのような情報を伝達することを違法にする制限を、自己が認識していること、そして、本契約の対象となる事項を知らされる代理人に忠告することを、表明する。

8. 従業員の非勧誘 各当事者は、本契約の期間中、及び、本契約の終了後2年間、直接又は他者を介して、当事者間で潜在的取引の評価中に接触した、相手方の従業員を、自身又はその関連会社の、従業員、コンサルタント、又は独立請負業者になるように、勧誘したり、勧誘しようとしたりしない。ただし、ここに含まれる規定は、各従業員の制限合意に準拠するものの、直接又は他者を介して、(i) そのような従業員を特に対象としない、一般的な勧誘を行うことを、禁止するものではない。疑義を避ける目的で記載すると、そのような一般的な広告に応答する、若しくは、他の当事者又はその関連会社の雇用を辞めるため、勧誘又は誘因なしに、そのような当事者又はその関連会社に近づく、他の当事者の従業員を、雇用又は採用することは、本条違反とはみなされない。(ii) 相手方又はその関連会社によって解雇された、相手方又はその関連会社の従業員を、雇用又は雇用に勧誘することを、禁止するものではない。

9. その他.

(a) 本契約は、本契約の主題に関連する、書面又は口頭による、当事者間の以前の全合意を置き換える。本契約は、当事者が署名した書面での合意による場合を除き、全体又は一部を、変更、改正、又は解除することはできない。

(b) 本契約は、本契約の当事者、及び、それぞれの相続人、後継者、譲受人の利益を拘束し、効力を生じる。

(c) 本契約は、準拠法の原則に影響を与えることなく、マサチューセッツ州内法に従って、解釈及び理解される。

(d) 本契約の規定は、当事者の事業及びのれんの保護に必要であり、当事者は、そのような目的のために、合理的であると見なす。受領者は、本契約の違反が、開示当事者に重大かつ取り返しのつかない損害をもたらすことに同意し、したがって、違反が発生した場合、利用可能な他の救済策に加えて、開示当事者は、特定の義務履行、その他、差止命令及び衡平法上の救済を求める権利を有する。

(e) 本契約によって課される秘密保持義務は、本契約に従って受領者に保有情報を開示してから5年間、保有情報の特定の項目に関して、継続する。ただし、保有情報に含まれるソースコードに関して、本契約により課せられる守秘義務は、永続的に継続するものとする。

(f) 当事者の便宜のために、本契約は、ファクシミリで締結することができ、契約書(2部)は、それぞれが原本と見なされ、一体として、両方の当事者を拘束する1つの契約を構成するものとする。

上記の年月日に、封印された書面として署名完了。

5 来訪者受付表

Visitor List

From [/ /] to [/ /]
Located at []
Attended by []
Reviewed by []

No.	Name	ID checked	Contact details	Affiliation	Arrival	Departure	Accepted by

(参考和訳)来訪者受付表

訪問者リスト

[/ /]から[/ /]まで
所在地 []
確認者 []
監督者 []

No.	氏名	本人確認	連絡先	所属組織	到着時刻	出発時刻	受入対応者 (受入先)

第2章 ドイツにおける参考書式

1 就業規則における秘密保護関連規定の例 German Staff Handbook

DATED

[EMPLOYER'S NAME]

STAFF HANDBOOK

Staff handbook

1. Introduction

1.1 [GENERAL DETAILS ABOUT THE EMPLOYER AND ITS BUSINESS.]

1.2 We are an equal opportunities employer and do not discriminate on the grounds of gender, sexual orientation, marital or civil partner status, pregnancy or maternity, gender reassignment, race, colour, nationality, ethnic or national origin, religion or belief, disability or age.

2. Using the Staff Handbook

2.1 This Staff Handbook sets out the main policies and procedures that you will need to be aware of while working for us. You should familiarise yourself with it and comply with it at all times. Any questions you may have with regard to its contents or what you have to do to comply with it should be referred to the Human Resources Department.

2.2 The policies and procedures set out in this handbook apply to all employees unless otherwise indicated. They therefore apply to managers, officers, directors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, casual and agency staff and volunteers (collectively referred to as **staff** in this handbook). They do **not** form part of the terms of your contract with us, which are provided to you separately.

2.3 Our policies and procedures have been agreed with the TRADE UNION **OR** WORKS COUNCIL.

3. Responsibility for the Staff Handbook

3.1 The HR Manager has overall responsibility for this Staff Handbook and for ensuring that its policies and procedures comply with our legal obligations.

3.2 The Staff Handbook is reviewed regularly to ensure that its provisions continue to meet our legal obligations and reflect best practice.

3.3 Everyone should ensure that they take the time to read and understand the content of this handbook and act in accordance with its aims and objectives. Managers must ensure all staff understand the standards of behaviour expected of them and to take action when behaviour falls below those requirements.

4. Personal data

Whenever we process personal data about you in connection with our policies, we will process it in accordance with our Data Protection Policy. We will only process your personal data if we have

a lawful basis for doing so. We will notify you of the purpose or purposes for which we use it. Please see the Privacy Notice on the intranet for further information.

5. Emergency contact details

The Human Resources Department is responsible for maintaining up-to-date details of your home address and the emergency contact telephone numbers of the person or persons you would like us to contact in the event of an emergency, for example if you have an accident. This information will be requested by the Human Resources Department when you start work and you should advise us of any changes straight away. This information is held in confidence and will only be used when needed.

Schedule 1 Disciplinary and Capability Procedure

1. About Procedure

- 1.1 This procedure is intended to help maintain standards of conduct and performance and to ensure fairness and consistency when dealing with allegations of misconduct or poor performance.
- 1.2 Minor conduct or performance issues can usually be resolved informally with your line manager. This procedure sets out formal steps to be taken if the matter is more serious or cannot be resolved informally.
- 1.3 This procedure applies to all employees regardless of length of service. It does not apply to agency workers or self-employed contractors.
- 1.4 This procedure does not form part of any employee's contract of employment and we may amend it at any time.

2. Investigations

- 2.1 Before any disciplinary hearing is held, the matter will be investigated. Any meetings and discussions as part of an investigation are solely for the purpose of fact-finding and no disciplinary action will be taken without a disciplinary hearing.
- 2.2 In some cases of alleged misconduct, we may need to suspend you from work while we carry out the investigation or disciplinary procedure (or both). [While suspended, you should not visit our premises or contact any of our clients, customers, suppliers, contractors or staff, unless authorised to do so.] Suspension is not considered to be disciplinary action.

3. Hearing

- 3.1 We will give you written notice of the hearing, including sufficient information about the alleged misconduct or poor performance and its possible consequences to enable you to prepare. You will normally be given copies of relevant documents and witness statements.
- 3.2 You may be accompanied at the hearing by a trade union representative or a colleague, who will be allowed reasonable paid time off to act as your companion.
- 3.3 You should let us know as early as possible if there are any relevant witnesses you would like to attend the hearing or any documents or other evidence you wish to be considered.
- 3.4 We will inform you in writing of our decision, usually within one week of the hearing.

4. Disciplinary Action and Dismissal

4.1 The usual penalties for misconduct or poor performance are:

- (a) **Stage 1: First written warning [or improvement note].** Where there are no other active written warnings [or improvement notes] on your disciplinary record, you will usually receive a first written warning [or improvement note]. It will usually remain active for six months.
- (b) **Stage 2: Final written warning.** In case of further misconduct or failure to improve where there is an active first written warning [or improvement note] on your record, you will usually receive a final written warning. This may also be used without a first written warning [or improvement note] for serious cases of misconduct or poor performance. The warning will usually remain active for 12 months.
- (c) **Stage 3: Dismissal or other action.** You may be dismissed for further misconduct or failure to improve where there is an active final written warning on your record, or for any act of gross misconduct. Examples of gross misconduct are given below (paragraph 6). You may also be dismissed without a warning for any act of misconduct or unsatisfactory performance during your probationary period.
- (d) We may consider other sanctions short of dismissal, including demotion or redeployment to another role (where permitted by your contract), and/or extension of a final written warning with a further review period.

5. Appeals

- 5.1 You may appeal in writing within three weeks of being told of the decision.
- 5.2 The appeal hearing will, where possible, be held by someone other than the person who held the original hearing. You may bring a colleague or trade union representative with you to the appeal hearing.
- 5.3 We will inform you in writing of our final decision as soon as possible, usually within one week of the appeal hearing. There is no further right of appeal.

6. Gross Misconduct

- 6.1 Gross misconduct will usually result in dismissal without warning, with no notice or payment in lieu of notice (summary dismissal).
- 6.2 Gross misconduct is a serious breach of contract and includes misconduct which, in our opinion, is likely to prejudice our business or reputation or irreparably damage the working relationship and trust between us. This may include misconduct committed outside of work. The following are examples of matters that are normally regarded as gross misconduct:
 - (a) theft or fraud;

- (b) physical violence or bullying;
- (c) deliberate and serious damage to property;
- (d) serious misuse of the organisation's property or name;
- (e) deliberately accessing internet sites containing pornographic, offensive or obscene material;
- (f) serious insubordination;
- (g) unlawful discrimination, victimisation or harassment;
- (h) bringing the organisation into serious disrepute;
- (i) serious incapability at work brought on by alcohol or illegal drugs;
- (j) causing loss, damage or injury through serious negligence;
- (k) a serious breach of health and safety rules;
- (l) a serious breach of confidence.

This list is intended as a guide and is not exhaustive.

Schedule 2 Grievance Procedure

1. Step 1: Written Grievance

- 1.1 You should put your grievance in writing and submit it to your line manager. If your grievance concerns your line manager you may submit it to [POSITION].
- 1.2 The written grievance should set out the nature of the complaint, including any relevant facts, dates, and names of individuals involved so that we can investigate it.

2. Step 2: Meeting

- 2.1 We will arrange a grievance meeting, normally within [one week] of receiving your written grievance. You should make every effort to attend.
- 2.2 We may adjourn the meeting if we need to carry out further investigations, after which the meeting will usually be reconvened.
- 2.3 We will, usually within two weeks of the last grievance meeting, issue our decision and notify you of any further action that we intend to take to resolve the grievance. We will also advise you of your right of appeal.

3. Step 3: Appeals

- 3.1 You may appeal in writing to us, stating your grounds of appeal, within three weeks of the date on which the decision was sent or given to you.
- 3.2 We will hold an appeal meeting, normally within four weeks of receiving the appeal. This will be dealt with impartially by three managers who have not previously been involved in the case.
- 3.3 We will confirm our final decision in writing, usually within two weeks of the appeal hearing. There is no further right of appeal.

Schedule 3 IT/Communications Policy

1. About Policy

- 1.1 Breach of this policy may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

2. Equipment Security

- 2.1 You are responsible for the security of the equipment allocated to or used by you, and you must not allow it to be used by anyone other than in accordance with this policy. You should use passwords on all IT equipment, particularly items that you take out of the office. You should keep your passwords confidential and change them regularly.
- 2.2 You may use the equipment allocated to you only to serve our business goals. You may not use the equipment for anything that does not support or augment our business.
- 2.3 You must only log on to our systems using your own username and password. You must not use another person's username and password or allow anyone else to log on using your username and password.
- 2.4 If you are away from your desk you should log out or lock your computer. You must log out and shut down your computer at the end of each working day.

3. Systems/Programs/Infrastructures

- 3.1 You should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of your duties).
- 3.2 You must not download or install software from external sources without authorisation from [POSITION]. Downloading unauthorised software may interfere with our systems and may introduce viruses or other malware.
- 3.3 You must not attach any device or equipment including mobile phones, tablet computers or USB storage devices to our systems without authorisation from [POSITION].
- 3.4 We monitor all e-mails passing through our system for viruses. You should exercise particular caution when opening unsolicited e-mails from unknown sources. If an e-mail looks suspicious do not reply to it, open any attachments or click any links in it.
- 3.5 Inform [POSITION] immediately if you suspect your computer may have a virus.

4. E-mail Communication

- 4.1 Adopt a professional tone and observe appropriate etiquette when communicating with third parties by e-mail. [You should also include our standard e-mail signature and disclaimer.]
- 4.2 Remember that e-mails can be used in legal proceedings and that even deleted e-mails may remain on the system and be capable of being retrieved.
- 4.3 You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate e-mails.
- 4.4 You should not:
 - (a) send or forward private e-mails at work which you would not want a third party to read;
 - (b) send or forward chain mail, junk mail, cartoons, jokes or gossip;
 - (c) contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to others who do not have a real need to receive them; or
 - (d) send messages from another person's e-mail address (unless authorised) or under an assumed name.
- 4.5 Do not use your own personal e-mail account to send or receive e-mail for the purposes of our business. Only use the e-mail account we have provided for you.
- 4.6 [We do not permit access to web-based personal e-mail such as Gmail or Hotmail on our computer systems at any time due to additional security risks.]

5. Internet

- 5.1 Internet access is provided solely for business purposes. [Occasional personal use may be permitted as set out in paragraph 6.]
- 5.2 You should not access any web page or download any image or other file from the internet which could be regarded as illegal, offensive, in bad taste or immoral. Even web content that is legal in Germany may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.
- 5.3 We may block or restrict access to some websites at our discretion.

6. Monitoring

- 6.1 Our systems enable us to monitor telephone, e-mail, voicemail, internet and other communications. For business reasons, and in order to carry out legal obligations in our role as an employer, your use of our systems including the telephone and computer systems (including any personal use) may be continually monitored by automated software or otherwise.
- 6.2 We reserve the right to retrieve the contents of e-mail messages or check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, including for the following purposes (this list is not exhaustive):
- (a) to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy;
 - (b) to find lost messages or to retrieve messages lost due to computer failure;
 - (c) to assist in the investigation of alleged wrongdoing; or
 - (d) to comply with any legal obligation.

7. Prohibited Acts

- 7.1 Misuse of our telephone or e-mail system or inappropriate internet use will be dealt with Disciplinary Procedure. Misuse of the internet can in some cases be a criminal offence.
- 7.2 Creating, viewing, accessing, transmitting or downloading any of the following material will usually amount to gross misconduct (this list is not exhaustive):
- (a) pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);
 - (b) offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our clients;
 - (c) a false and defamatory statement about any person or organisation;
 - (d) material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Equal Opportunities Policy or our Anti-harassment and Bullying Policy);
 - (e) confidential information about us or any of our staff or clients (except as authorised in the proper performance of your duties);
 - (f) unauthorised software;
 - (g) any other statement which is likely to create any criminal or civil liability (for you or us); or
 - (h) music or video files or other material in breach of copyright.

(参考和訳)就業規則における秘密保護関連規定の例
ドイツ 就業規則

日付

[雇用主の名称]

就業規則

就業規則

1. 序文

1.1 [雇用主とその事業に関する概括的な説明]

- 1.2 当社は、機会均等を目指す雇用主であり、性別、性的指向、婚姻若しくは市民権のパートナーの地位、妊娠若しくは出産、性別の再割当て、人種、肌の色、国籍、民族、若しくは、出身国、宗教若しくは信念、障害、又は、年齢を理由に、差別しない。

2. 就業規則の使用

- 2.1 本就業規則は、あなたが、当社のために働いている間、あなたが知っておく必要がある、主要な方針や手続きを示す。あなたは、これに精通し、常に、従わないとならない。この内容、あるいは、これを遵守するためにあなたがしなければならないことに関して、あなたが持つ疑問については、人事部に照会されるべきである。
- 2.2 このハンドブックに記載されている方針及び手順は、特に明記されていない限り、すべての従業員に適用される。したがって、これらは、マネージャー、役員、取締役、従業員、コンサルタント、請負業者、研修生、在宅勤務者、パートタイム、並びに、有期労働者、臨時スタッフ、並びに、代理店のスタッフ、及び、ボランティア（このハンドブックでは、まとめて「従業員」と呼ぶ。）に適用される。これらは、別途提供される、当社との契約条件の一部を構成するものではない。
- 2.3 この方針及び手順は、労働組合[または労使協議会]と合意されている。

3. 就業規則への責任

- 3.1 人事部長は、この従業員ハンドブックに対して、全体的な責任を負い、その方針及び手順が、当社の法的義務に準拠していることを確認する。
- 3.2 スタッフハンドブックは定期的に見直され、その規定が、引き続き当社の法的義務を果たし、ベストプラクティスを反映しているか、確認される。
- 3.3 各従業員は、時間をかけ、このハンドブックの内容を読んで理解し、その目標と目的に従って行動する。管理者は、全従業員が、彼らに期待される行動の基準を理解し、行動がその基準を下回ったときに、確実に対処しなければならない。

4. 個人情報

当社の方針に関連して、あなたの個人データを処理する場合は、常に、データ保護ポリシーに従って処理される。あなたの個人データは、法的基礎がある場合にのみ、処理され、あなたに当社の使用目的が知らされる。詳細については、イントラネットのプライバシー通告を参照するものとする。

5. 緊急連絡先

人事部は、自宅の住所、及び、事故などの緊急時に、当社に連絡を取らせたい緊急連絡先の電話番号の、最新情報の詳細を維持する責任がある。これらの情報は、あなたが職務を開始するときに、人事部から要求され、定期的に、これらが最新であることを確認するように求められる。この情報は機密情報として保持され、必要な場合にのみ使用される。

Schedule 1 懲戒手続及び職能手続

1. 手順について

- 1.1 この手順は、行動及びパフォーマンスの基準を維持し、不正行為や業績の低下の申立てに対処する際の、公平性及び一貫性を確保することを目的とする。
- 1.2 軽微な行動やパフォーマンスの問題は、通常、ラインマネージャーと非公式に解決できる。この手順は、問題がより深刻であるか、非公式に解決できない場合に取りられるべき正式な手順を示している。
- 1.3 この手順は、勤続期間に関係なくすべての従業員に適用されます。派遣労働者や自営業の請負業者には適用されません。
- 1.4 この手順は、従業員の雇用契約の一部を構成するものではなく、当社はいつでも改変することができる。

2. 調査

- 2.1 懲戒審問が開かれる前に、問題が調査されます。当該調査の一環としての会議や話し合いは、事実を明らかにすることのみを目的としており、審問が行われることなく懲戒処分が行われることはない。
- 2.2 逸脱行為が疑われる場合、調査または懲戒手続（あるいはその両方）の間、あなたは業務を中止しなければならない可能性がある。[停職中は、許可されていない限り、当社施設を訪問したり、クライアント、顧客、納入業者、請負業者、スタッフに連絡してはならない。]停職は、懲戒処分とは見なされない。

3. 審問

- 3.1 審問は、申し立てられた逸脱行為又は業績の低下、及び、考えられる結果に関して、準備を可能にする十分な情報を含めて、当社があなたに書面で通知する。通常、関連する書類及び証人陳述書のコピーが渡される。
- 3.2 審問には、労働組合の代表者又は同僚が、あなたに同席することができる。同僚は、あなたの同伴者として行動するために、合理的な有給休暇を与えられる。
- 3.3 審問に出席させたい関連する証人、または検討したい文書やその他の証拠がある場合は、できるだけ早くお知らせください。
- 3.4 決定は、審問から通常1週間以内に書面で通知される。

4. 懲戒処分と解雇

- 4.1 逸脱行為又は業績低下に対する通常の罰則は、以下のとおりである：

- (a) **第1段階：第一警告状[又は、改善通告].** 他の有効な警告状[又は、改善通告]があなたの懲戒記録に無い場合、あなたは、通常第一警告状[又は、改善通告]を受け取る。それは、6ヶ月間有効に存続する。
- (b) **第2段階：最終警告状.** 有効な第一警告状[又は、改善通告]があなたの懲戒記録に存在し、さらなる逸脱行動又は改善の欠如がある場合、あなたは、通常最終警告状を受け取る。重大な逸脱行為又は業績不良の場合には、第一警告状[又は、改善通告]なく、これを使用されても良い。この警告状は、12ヶ月間有効に存続する。
- (c) **第3段階：解雇又は他の処分.** 最終警告状があなたの懲戒記録に存在し、さらなる逸脱行動又は改善の欠如がある場合、又は、重大な逸脱行動がある場合、あなたは、解雇となりうる。重大な逸脱行為の例は、以下(6)がある。また、試用期間中の逸脱行為や不満足な業績について、警告なしに解雇されうる。
- (d) 降格または別の役割への再配置（契約で許可されている場合）、及び/又は、さらなる見直し期間を伴う、最終的な書面による警告の延長を含む、解雇に至らない他の制裁を検討する場合がある。

5. 不服申立て

- 5.1 決定を受けてより3週間以内に、不服申立てをすることができる。
- 5.2 不服申立ての審問は、可能であれば、原審問に関与した者以外の者によって、行われる。同僚又は労働組合の代表者を、不服申立ての審問に、連れて行くことができる。
- 5.3 最終決定については、できるだけ早く、通常は、不服申立審理から、1週間以内に書面で通知される。それ以上に、不服申立てを行う権利はない。

6. 重大な逸脱行為

- 6.1 重大な逸脱行為は通常、警告なしに解雇され、通告、又は、通告の代わりに支払いが行われない（要約解雇）。
- 6.2 重大な逸脱行為は、重大な契約違反であり、私たちの意見では、私たちのビジネスや評判を損なうか、当社の仕事上の関係や信頼を、取り返しのつかないほど損なう可能性のある逸脱行為が含まれる。これには、仕事以外で行われた逸脱行為が含まれうる。以下が、通常、重大な逸脱行為と見なされる件の例である。：
 - (a) 窃盗または詐欺；
 - (b) 身体的暴力またはいじめ；
 - (c) 財物への故意かつ重大な損傷；
 - (d) 組織の財物または名前の重大な誤用；
 - (e) ポルノ、攻撃的、又は、わいせつな素材を含むインターネットサイトに故意にアクセスすること；
 - (f) 深刻な不服従；

- (g) 違法な差別、危害、嫌がらせ；
- (h) 組織を深刻な不評に陥れること；
- (i) アルコールまたは違法薬物によって引き起こされた、職場での深刻な能力欠如；
- (j) 重大な過失により損失、損傷、又は傷害を引き起こすこと；
- (k) 健康と安全に関する規則の重大な違反；
- (l) 重大な守秘義務違背；

このリストは、ガイドとして意図されており、網羅的なものでない。

Schedule 2 苦情処理

1. Step 1: 書面による苦情

- 1.1 苦情を書面で提出し、ラインマネージャーに提出する必要がある。あなたの苦情があなたのラインマネージャーに関係しているなら、あなたはそれを[]に提出することができる。
- 1.2 書面による苦情は、調査できるように、関連する事実、日付、関係者の名前など、苦情の性質を記載する必要がある。

2. Step 2: 会議

- 2.1 苦情処理会議は、通常、書面による苦情を受け取ってから[1 週間]以内に、開催される。あなたが出席できるよう、あらゆる努力をしなければならない。
- 2.2 会議は、更に調査を行う必要がある場合、延期されることがある。その後、会議は、通常再開される。
- 2.3 通常、最後の苦情処理会議から 2 週間以内に、決定を下し、苦情を解決するために取られる、さらなる措置について通知する。また、不服申立権についても通知される。

3. Step 3: 不服申立て

- 3.1 あなたは、決定があなたに送られた、または与えられた日から 3 週間以内に、あなたの不服の理由を書面で訴えることができる。
- 3.2 通常、不服申立てを受けてから、4 週間以内に、不服申立会議を開催する。これは、それまで事件に関与したことの無い 3 人のマネージャーによって、公平に処理される。
- 3.3 最終決定は、書面で確認する。通常、不服申立審理から 2 週間以内になされる。それ以上の不服申立権はない。

Schedule 3 IT 及び通信システム方針

1. 本方針

- 1.1 この方針の違反は、懲戒手続で対応される可能性があり、深刻な場合には、即時解雇につながる重大な逸脱行為として扱われる可能性がある。

2. 機器の安全性

- 2.1 あなたは、あなたに割り当てられた、または、あなたが使用する機器の安全性に責任を負い、この方針に服する者以外の者による使用を許可してはならない。すべての IT 機器、特に、オフィスから持ち出す品目には、パスワードを使用しなければならない。パスワードは、内密にし、定期的に変更する必要がある。
- 2.2 割り当てられた機器は、当社のビジネス目標を達成するためにのみ、使用できる。当社の事業の支持または発展以外の目的で、機器を使用してはならない。
- 2.3 自分のユーザー名及びパスワードを使用してのみ、システムにログオンしなければならない。他人のユーザー名及びパスワードを使用したり、他人に、自分のユーザー名及びパスワードを使用してログオンさせたりしてはならない。
- 2.4 端末から離れている場合は、ログアウトするか、コンピューターをロックする。終業時には、ログアウトして、コンピューターをシャットダウンしなければならない。

3. システム/プログラム/基盤

- 3.1 既存のシステム、プログラム、情報若しくはデータを、削除、破棄、又は変更してはならない（職務の適切な遂行において、特別に許可されている場合を除く。）。
- 3.2 []の許可なしに、外部ソースからソフトウェアをダウンロード、又はインストールしてはならない。許可されていないソフトウェアをダウンロードすると、システムに影響を与え、ウイルスやその他のマルウェアを導入する可能性がある。
- 3.3 []の許可なしに、携帯電話、タブレットコンピューター、USB ストレージデバイス等のデバイスを、システムに接続してはならない。
- 3.4 システムを通過する、すべての電子メールを、そのウイルス感染について監視する。送信元不明の迷惑メールを開く場合は、特に注意すること。電子メールが疑わしいと考える場合には、返信、添付ファイル開封、及びその中のリンクをクリック、をいずれもしてはならない。
- 3.5 コンピュータにウイルスまたはマルウェアが含まれている可能性がある場合は、直ちに []に通知する。

4. E-mail

- 4.1 電子メールで第三者とコミュニケーションをとるときは、業務上の口調を採用し、適切なエチケットに沿ったものとする。[標準の電子メール署名と、免責事項も含める必要がある。]
- 4.2 電子メールは、法的手続で使用でき、削除された電子メールもシステムに残り、取り寄せる可能性があることに注意する。
- 4.3 虐待的、わいせつな、差別的、人種差別的、嫌がらせの、侮蔑的、中傷的、性的表現の、又は、その他不適切な電子メールを送信してはならない。
- 4.4 以下は禁止される：
 - (a) 第三者に読まれたくない、職場の内密な電子メールを送信、又は転送する。
 - (b) チェーンメール、ジャンクメール、漫画、ジョーク、ゴシップを、送信、又は転送する。
 - (c) 些細なメッセージを送信したり、実際に受信する必要のない他者に、電子メールを不必要にコピー、又は転送したりすることで、システム混雑に加担する。
 - (d) 他者の電子メールアドレス（許可されていない場合）又は仮名で、メッセージを送信する。
- 4.5 当社の業務目的で電子メールを送受信するために、あなた自身の個人的な電子メールアドレスを使用してはならない。提供された電子メールアドレスのみを使用しなければならない。
- 4.6 [追加のセキュリティリスクのため、Gmail や Hotmail などの Web ベースの個人用電子メールへのアクセスをコンピューターシステムでいつでも許可していない。]

5. インターネット

- 5.1 インターネットへのアクセスは、業務目的のみに付与されている。[時折の個人使用は、第 6 項に記載のように、許される。]
- 5.2 違法、攻撃的、悪趣味、又は不道德と見なされる可能性のある、Web ページにアクセスしたり、インターネットから画像やその他のファイルをダウンロードしたりしてはならない。ドイツ内で合法である Web コンテンツであっても、この禁止事項に該当する程度に悪趣味である可能性が存在する。原則として、（ページを表示することを意図しているかどうかにかかわらず）誰かがページのコンテンツに当惑する可能性がある場合、又は、当社のソフトウェアが、ページまたはファイルにアクセスしたという事実が公開された場合、問題となる可能性がある場合、当該表示が、この方針違反となる。
- 5.3 当社の裁量で、いくつかのウェブサイトブロックしたり、アクセス制限したりすることがある。

6. 監視

6.1 当社のシステムは、電話、電子メール、ボイスメール、インターネット、その他の通信を監視することができる。業務上の理由から、また、雇用主としての当社の役割から、法的義務を遂行するために、電話及びコンピューターシステムを含む、当社のシステムの使用（個人的な使用を含む。）は、自動ソフトウェア又はその他の方法で、継続的に監視される場合がある。

6.2 当社は、以下の目的を含め、業務上の利益のために合理的に必要な場合、電子メールメッセージの内容を取り寄せしたり、インターネットの使用状況（アクセスしたページや行われた検索を含む。）を確認したりする権利を留保する（このリストは網羅的ではない。）。

(a) 電子メールシステムまたはインターネットの使用が合法であり、このポリシーに準拠しているかどうかを監視するため。

(b) 失われたメッセージを検索するため、又は、コンピューターの障害のために失われたメッセージを取得するため。

(c) 申し立てられた不正行為の調査を支援するため。

(d) 法的義務を遵守するため。

7. 禁止事項

7.1 当社の電話又は電子メールシステムの誤用、若しくは、不適切なインターネットの使用は、懲戒手続で対応する。インターネットの誤用は、場合によっては、犯罪となる可能性がある。

7.2 次の資料の作成、表示、アクセス、送信、又はダウンロードは、通常、重大な逸脱行為となる（このリストは網羅的ではない。）。

(a) ポルノ素材（つまり、性的に露骨または興奮する性質の文章、写真、映画、ビデオクリップ）；

(b) 攻撃的、わいせつ、又は犯罪的な内容、若しくは、当社又はクライアントに当惑を引き起こす可能性のある内容。

(c) 個人又は組織に関する、虚偽の名誉毀損の声明。

(d) 差別的、攻撃的、侮蔑的、又は他者を当惑させる可能性のある資料（機会均等ポリシー、ハラスメント防止、及びいじめに関するポリシーに違反する資料を含む）。

(e) 当社、当社のスタッフ又はクライアントに関する機密情報（職務の適切な遂行において許可されている場合を除く。）。

(f) 許可されていないソフトウェア。

- (g) (あなた又は当社にとって) 刑事または民事責任を引き起こす可能性のあるその他の声明。
- (h) 著作権を侵害する音楽、ビデオファイル又はその他の素材。

2 従業員との秘密保持契約書の例

Annex 2 – Confidentiality Clause in Employment Contract

§ 1 Geheimhaltung und Rückgabe von Unterlagen

(1) Der Arbeitnehmer ist verpflichtet, insbesondere auch während der Zeit nach Beendigung dieses Arbeitsvertrages alle vertraulichen Angelegenheiten, Betriebs- und Geschäftsgeheimnisse des Arbeitgebers und verbundener Unternehmen, welche ihm bei Ausübung seiner Tätigkeiten für den Arbeitgeber zur Kenntnis gelangen (insbesondere Verfahren, Daten, Know-how, Marketing-Pläne, Geschäftsplanungen, unveröffentlichte Bilanzen, Budgets, Lizenzen, Preise, Kosten und Kunden- und Lieferantenlisten) oder die vom Arbeitgeber als vertraulich bezeichnet werden, streng geheim zu halten.

(2) Bei Beendigung des Arbeitsverhältnisses oder bei Freistellung wird der Arbeitnehmer dem Arbeitgeber unaufgefordert, während des Bestehens seines Arbeitsverhältnisses auf Anforderung, alle in seinem Besitz befindlichen, den Arbeitgeber oder die Verbundenen Unternehmen betreffenden Unterlagen und Datenträger, insbesondere alle Notizen, Berichte, Memoranden, Aufzeichnungen, Akten, Zeichnungen, Protokolle und andere ähnliche Dokumente (sowie Kopien oder sonstige Reproduktionen hiervon) zurückgeben.

(3) Der Arbeitnehmer erkennt an, dass die vorgenannten Unterlagen alleiniges Eigentum des Arbeitgebers oder der Verbundenen Unternehmen sind. Der Arbeitnehmer hat an den genannten Unterlagen kein Zurückbehaltungsrecht.

§ 1 Confidentiality and Return of Documents

(1) During and after the term of this Employment Agreement, the Employee shall treat as strictly confidential all confidential matters and trade and business secrets of the Employer and all Affiliated Companies, of which he/she obtains knowledge during the exercise of his/her duties for the Employer (including procedures, data, know-how, marketing plans, business planning, unpublished balance sheets, budgets, licenses, pricing, costs and customer and supplier lists) or which are designated as confidential by the Employer.

(2) The Employee shall, upon termination of the employment or in the event of the Employee being released from his/her duties, without being asked, and during the existence of his/her employment, upon request, return to the Employer all documents and data carriers in his/her possession which relate to the Employer or to any Affiliated Company including notes, reports, memoranda, records, files, drawings, protocols and other similar documents (as well as copies or other reproductions thereof).

(3) The Employee acknowledges that the documents referred to above are the sole property of the Employer or any Affiliated Company. The Employee has no right of retention regarding these documents.

(4) Veröffentlichungen und Vorträge des Arbeitnehmers während der Dauer des Arbeitsverhältnisses bedürfen der vorherigen Zustimmung des Arbeitgebers, soweit diese die Branche, Erzeugnisse oder Dienstleistungen des Arbeitgebers betreffen. Die Zustimmung ist zu erteilen, wenn keine gemäß Absatz (1) geheimhaltungsbedürftigen Tatsachen mitgeteilt und auch ansonsten keine schützenswerten Interessen des Arbeitgebers verletzt werden. (alternativ: Dem Arbeitnehmer ist es gestattet, Fachvorträge zu halten und unter eigenem Namen zu veröffentlichen. Die Verschwiegenheitspflicht gemäß Absatz (1) bleibt unberührt.)

(4) Any publications and lectures of the

§ 2 Datensicherheit

(1) Das Kopieren von Daten und/oder Software auf mobile Datenträger ist verboten, soweit nicht in Textform durch den Arbeitgeber gestattet. Der Arbeitnehmer hat ist verpflichtet, bei Verlassen seines Arbeitsplatzes seinen Computer gegen unbefugte Zugriffe zu sperren.

(2) Der Arbeitnehmer ist verpflichtet, alle betriebsbezogenen Daten nur auf dem vom Arbeitgeber zugewiesenen Serververzeichnis abzulegen. Die Speicherung von Daten auf Desktoprechnern ist aus Schutz- und Sicherheitsgründen vermieden werden.

(2) The employee is obliged to store all

(3) Der Arbeitnehmer ist im Rahmen der allgemeinen Sorgfaltspflichten für den Schutz der auf einem dezentralen Rechner befindlichen Daten verantwortlich. Dies gilt insbesondere für Daten auf Notebooks.

Employee during the term of the employment require the prior consent of the Employer in so far as such publications and lectures concern the branch, products or services of the Employer. The Employer shall grant such consent if no information required to be kept confidential as described in para. (1) will be disclosed, and no other interests of the Employer which deserve protection are disregarded. (alternatively: The Employee may give professional lectures and publish under his/her own name. The confidentiality obligation pursuant to para. (1) remains unaffected.)

§ 2 Data Security

(1) The copying of data and/or software to mobile data carriers is prohibited unless permitted in text form by the employer. The employee is obliged to lock his computer against unauthorised access when leaving his workplace.

company-related data only on the server directory assigned by the employer. The storage of data on desktop computers shall be avoided for reasons of protection and security.

(3) Within the general duties of care, the employee shall be responsible for the protection of data located on a decentralised computer. This applies in particular to data on notebooks.

(4) Der Arbeitgeber stellt sicher, dass der Arbeitnehmer in einer für die jeweilige Aufgabenstellung gesicherten Arbeitsumgebung arbeitet, also entsprechende Programme und Geräte zur Verschlüsselung bzw. Sicherung werden zur Verfügung gestellt. Der Arbeitnehmer ist verpflichtet, die zur Verfügung gestellten Sicherungsmittel zu nutzen.

(5) Die Verwendung privater Geräte und Speicher für betriebsgezogene Tätigkeiten ist unzulässig. Sofern der Arbeitgeber mobile Geräte und Speicher (z.B. USB- Sticks) ausgibt, sind ausschließlich diese zulässig und dürfen ausschließlich mit betrieblichen Computern verwendet werden.

(4) The employer shall ensure that the employee works in a secured working environment for the respective task, i.e. appropriate programmes and devices for encryption or backup shall be provided. The employee is obliged to make use of the security devices provided.

(5) The use of private devices and storage devices for business-related activities is not permitted. If the employer issues mobile devices and storage devices (e.g. USB drives), only these are permitted and may only be used with company computers.

(参考和訳)従業員との秘密保持契約書の例

雇用契約中の秘密保持義務

§ 1 機密保持と返還

- (1) 本雇用契約の期間中及び終了後、従業員は、自己の職責を遂行する際に知ることとなった、又は、雇用主から機密情報として指定されている、雇用主とすべての関係会社の機密事項と事業秘密および営業秘密のすべて（手順、データ、ノウハウ、マーケティング計画、事業計画、未発表の貸借対照表、予算、ライセンス、価格設定、コスト、顧客、および納入者リストを含む。）を、機密として厳格に扱う。
- (2) 従業員は、雇用終了時又は離職の求めの際、要請されるまでもなく、及び、雇用中、要請に応じて、雇用主または関連会社に関連する、所有しているすべての文書及びデータ伝送手段（ノート、レポート、メモ、記録、ファイル、図面、プロトコル、及び、その他の同様の文書、並びに、そのコピーや複製も含む。）を雇用主に返還する。
- (3) 従業員は、上記の文書は、雇用主または関連会社だけの財産であり、従業員が、これら文書に関して保持する権利はないことを認める。
- (4) 従業員が、雇用期間中に行う発表や講演には、そのような発表や講義が、雇用主の支部、製品又はサービスに関係する限り、雇用主の事前の同意が必要となる。雇用主は、前(1)項に記載されたような機密とすべき情報が、開示されることがなく、保護に値する雇用主の他の利益が損なわれることがない場合、そのような同意を与えるものとする。
- (5) [従業員は、自己の名前で専門的な講義を行い、発表することができる。但し、従業員の、前(1)項の守秘義務は、変更がない。]

§ 2 データ安全性

- (1) 雇用主によって文書で許可されていない限り、モバイルデータキャリアへ、データ及び/またはソフトウェアのコピーは禁止される。従業員は、職場を離れるとき、不正アクセスに対応し、コンピューターをロックする義務を負う。
- (2) 従業員は、会社関連のデータはすべて、雇用主によって割り当てられたサーバーディレクトリへ保管する義務を負う。デスクトップコンピューターへのデータの保存は、保護及びセキュリティの理由から、避けるようにする。
- (3) 従業員は、分散型コンピューターにあるデータの保護に、一般的な注意義務の範囲内で、責任を負う。これは、ノートブックのデータに、特に適用される。
- (4) 雇用主は、従業員が、それぞれの作業のための安全な環境、すなわち、適切なプログラムと装置の暗号化又はバックアップの提供をするものとする。従業員は、提供されるセキュリティデバイスの使用をする義務がある。
- (5) ビジネス関連の活動に、私的なモバイル装置や保存装置を使用することは許可されていない。雇用主が、モバイル装置と保存装置（USB ドライブなど）を提供する場合、これらのみが許可されており、会社のコンピューターに使用できる。

Annex 3 – Employer-employee non-compete agreement after resignation

§1 Für die Dauer von [•] Monaten nach Beendigung des Arbeitsverhältnisses ist es dem Arbeitnehmer untersagt, mit dem Arbeitgeber in Wettbewerb zu treten („Wettbewerbsverbot“).

§2 Das Wettbewerbsverbot bezieht sich
- sachlich auf alle Bereiche, in denen der Arbeitgeber zu dem Zeitpunkt, in dem das Arbeitsverhältnis endet, tätig ist und
- räumlich auf das gesamte Tätigkeitsgebiet des Arbeitgebers zu dem Zeitpunkt, in dem das Arbeitsverhältnis endet.
Sachlicher und räumlicher Geltungsbereich des Wettbewerbsverbots werden zusammenfassend als „Geschäftsbereich“ bezeichnet.

§ 3 Das Wettbewerbsverbot umfasst jegliche Wettbewerbstätigkeit im Geschäftsbereich des Arbeitgebers, sei es direkt oder indirekt, selbständig, als freier Mitarbeiter, arbeitnehmerähnlich oder als Arbeitnehmer/Angestellter, durch Errichtung eines oder Beteiligung an einem Wettbewerbsunternehmen, durch beratende Tätigkeiten oder auf sonstige Weise.

§ 4 Der Arbeitgeber verpflichtet sich, dem Arbeitnehmer für die Dauer des Wettbewerbsverbots eine Karenzentschädigung zu zahlen, die für jedes Jahr des Verbots die Hälfte der vom Arbeitnehmer zuletzt bezogenen vertragsmäßigen Leistungen erreicht. Anderweitigen Erwerb muss sich der Arbeitnehmer
§ 4 The employer undertakes to pay the

§1 For a period of [•] months after termination of the employment relationship, the employee is prohibited from competing with the employer ("non-competition obligation").

§2 The non-competition obligation relates
- materially to all areas in which the employer is active at the time the employment relationship ends and
- territorially to the employer's entire area of activity at the time the employment relationship ends.
The material and territorial scope of the non-competition obligation are collectively referred to as the "business area".

§ 3 The non-competition obligation includes any competitive activity in the employer's business area, whether directly or indirectly, self-employed, as a freelancer, quasi-employee or as an employee/employee, through the establishment of or participation in a competitive company, through advisory activities or in any other way.

employee for the duration of the noncompetition obligation a waiting allowance equal to half of the contractual benefits last received by the employee for each year of the non-competition obligation.

gemäß § 74c HGB anrechnen lassen. Der Arbeitnehmer ist verpflichtet, unaufgefordert spätestens am Schluss eines jeden Kalendervierteljahres anzugeben, ob und in welcher Höhe er anderweitige Einkünfte bezieht. Auf Verlangen hat der Arbeitnehmer die Angaben zu belegen.

§ 5 Das Wettbewerbsverbot gilt auch mit einem Rechtsnachfolger des Betriebs, insbesondere geht es bei einer Veräußerung auf den Erwerber über. Der Arbeitnehmer ist mit dem Übergang seiner Rechte aus dieser Vereinbarung einverstanden.

§ 6 Der Arbeitgeber kann vor Beendigung des Arbeitsverhältnisses durch schriftliche Erklärung auf das Wettbewerbsverbot mit der Wirkung verzichten, dass er mit Ablauf eines Jahres seit der Erklärung von der Verpflichtung frei wird, die Karenzentschädigung zu zahlen.

§ 7 Das nachvertragliche Wettbewerbsverbot tritt nur in Kraft, wenn das Arbeitsverhältnis vom Arbeitgeber oder Arbeitnehmer nicht vor Ablauf der Probezeit gekündigt wird. Das nachvertragliche Wettbewerbsverbot tritt nicht in Kraft, wenn das Arbeitsverhältnis aufgrund Eintritts in den Ruhestand endet.

§ 8 Verstößt der Arbeitnehmer schuldhaft gegen das Wettbewerbsverbot, ist er verpflichtet, eine Vertragsstrafe in Höhe des letzten Bruttomonatsgehalts zu zahlen.

The employee must take into account any other earnings pursuant to section 74c HGB. The employee is obliged to declare, without being asked, at the latest at the end of each calendar quarter, whether and to what extent he receives other income. Upon request, the employee shall provide evidence of the information.

§ 5 The non-competition obligation shall also apply with a legal successor of the business, in particular it shall pass to the acquirer in the event of a sale. The employee agrees to the transfer of his rights under this agreement.

§ 6 The employer may, before termination of the employment relationship, waive the non-competition obligation by written declaration with the effect that he shall be released from the obligation to pay the waiting compensation upon expiry of one year from the declaration.

§ 7 The post-contractual non-competition obligation shall only enter into force if the employment relationship is not terminated by the employer or the employee before the end of the probationary period. The post-contractual non-competition obligation shall not enter into force if the employment relationship ends due to retirement.

§ 8 If the employee culpably violates the non-competition obligation, he shall be obliged to pay a contractual penalty in the amount of the last gross monthly salary.

Besteht die Verletzungshandlung in der kapitalmäßigen Beteiligung an einem Wettbewerbsunternehmen oder der Eingehung eines Dauerschuldverhältnisses (zB Arbeits-, Dienst-, Handelsvertreter oder Beraterverhältnis), wird die Vertragsstrafe für jeden angefangenen Monat, in dem die kapitalmäßige Beteiligung oder das Dauerschuldverhältnis besteht, neu verwirkt (Dauerverletzung). Mehrere Verletzungshandlungen lösen jeweils gesonderte Vertragsstrafen aus, gegebenenfalls auch mehrfach innerhalb eines Monats. Erfolgen dagegen einzelne Verletzungshandlungen im Rahmen einer Dauerverletzung, sind sie von der für die Dauerverletzung verwirkten Strafe mit umfasst. Werden mehrere Vertragsstrafen verwirkt, ist der Gesamtbetrag der zu zahlenden Vertragsstrafen auf das Sechsfache des letzten Bruttomonatsgehalts begrenzt.

Die Geltendmachung von Schäden, die über die verwirkte Vertragsstrafe hinausgehen, bleibt vorbehalten. Vorbehalten bleibt auch die Geltendmachung aller sonstigen gesetzlichen und vertraglichen Ansprüche und Rechtsfolgen aus einer Verletzung (zB Unterlassungsansprüche, Wegfall des Anspruchs auf Karenzentschädigung für die Dauer des Verstoßes usw).

§ 9 Im Übrigen gelten die einschlägigen Vorschriften der §§ 74 ff HGB.

If the act of violation consists of a capital participation in a competitor company or of entering into a continuing obligation (e.g. employment, service, commercial agent or consulting relationship), the contractual penalty shall be forfeited anew for each month or part thereof during which the capital participation or the continuing obligation exists (continuing violation). Several acts of infringement each trigger separate contractual penalties, if necessary also several times within one month. If, on the other hand, individual acts of infringement occur within the scope of a continuing infringement, they are included in the penalty forfeited for the continuing infringement. If several contractual penalties are forfeited, the total amount of the contractual penalties to be paid is limited to six times the last gross monthly salary.

The right to claim damages in excess of the forfeited contractual penalty is reserved. The right to assert all other statutory and contractual claims and legal consequences arising from a violation (e.g. injunctive relief, forfeiture of the right to compensation for waiting for the duration of the violation, etc.) is also reserved.

§ 9 In all other respects, the relevant provisions of §§ 74 ff HGB shall apply.

雇用終了後の競業禁止義務

§ 1 雇用関係の終了後[・]か月間、従業員は、雇用主と競争することを禁じられている（「競業禁止義務」）。

§ 2 競業禁止義務は、以下に関わる。

- 雇用関係が終了した時点で、雇用主が活動しているすべての分野に、要素的に
 - 雇用関係が終了した時点の、雇用主の活動領域全体に、地理的に
- 競業禁止義務の要素と地理の範囲は、総して、「事業領域」と呼ばれる。

§ 3 競業禁止義務には、直接または間接を問わず、自営業者、フリーランサー、準従業員、又は従業員/従業員として、競争相手の設立または参加を通じて、助言活動を通じて、若しくは、他の方法で、雇用主の事業領域で競争する行為を含む。

§ 4 雇用主は、非競争義務の期間中の従業員に、競業禁止義務が課される毎年、当該従業員が最後に受け取った、契約上の利益の半分に等しい待機手当を支払うことを、約束する。

従業員は、HGB 第 74c 条に基づく、その他の収益を考慮に入れないとならない。従業員は、遅くとも各暦四半期の終わりに、質問されることなくとも、自己のその他の収益・収入を、受け取るかどうか、そしてどの程度受け取るか宣言する義務がある。従業員は、要求に応じて、情報の証拠を提供する。

§ 5 競業禁止義務は、ビジネスの法的な後継者にも適用され、特に、それは、ビジネス売却の場合の取得者に移される。従業員は、本合意により、自分の権利の譲渡に同意する。

§ 6 雇用主は、雇用関係が終了する前に、競業禁止義務を放棄する旨、そのような効果を伴う書面による宣言をして、宣言の 1 年経過から、待機中の補償を支払う義務から解放されることができる。

§ 7 契約後の競業禁止義務は、試用期間が終了する前に、雇用者または従業員が雇用関係を終了しなかった場合にのみ、発効する。

契約後の競業禁止義務は、退職により雇用関係が終了する場合、義務は発効しない。

§ 8 従業員が競業禁止義務に有責に反した場合、最後の月給総額を、契約上の罰金として支払う義務がある。

違反行為が競合企業への資本参加または継続的な義務を伴う（雇用、サービス、商業代理店、コンサルティング関係など）合意の締結である場合、契約上の罰金は、資本参加または継続的な義務（継続的違反）が存在する毎月又はその一部について、新たに徴収される。いくつかの侵害行為は、必要な場合、1 か月内に数回、それぞれ個別の契約上の罰金をもたらす。

一方、個々の侵害行為が継続的侵害の範囲内で発生した場合、それらは継続的侵害に対して徴収される罰金に含まれる。複数の契約上の罰金が徴収された場合、支払われる契約上のペナルティの合計額は、最後の月給総額の6倍に制限される。

徴収された契約上の罰金を超える、損害賠償を請求する権利は留保される。他の、すべての法定および契約上の請求、並びに、違反から生じる、法的な権利主張（例：差止めによる救済、違反の期間について雇用待機に対する補償の権利の没収など）も留保される。

§ 9 その他の全ての点で、HGB §§ 74 ffの規定が適用になる。

4 取引先との秘密保持契約書の例

Annex 4 – Confidentiality agreement with a business partner or customer

§ 1 Zusammenarbeit

(1) [Beschreibung der Geschäftsbeziehung der Parteien] (die „Zusammenarbeit“)

(2) Mit der vorliegenden Vereinbarung erhält jeder Vertragspartner Schutz für die Informationen, die im Rahmen dieser Zusammenarbeit schon weitergegeben wurden und noch weitergegeben werden.

§ 2 Vertrauliche Informationen

(1) Vertrauliche Informationen im Sinne dieser Vereinbarung sind alle Informationen, die

a) seitens eines Vertragspartners ausdrücklich und schriftlich als vertraulich bezeichnet wurden;

b) zu den nach §§ 17, 18 UWG geschützten Informationen gehören, insbesondere Know-how;

c) durch gewerbliche und andere Schutzrechte geschützt sind, zB Entwurfsmaterial für Software (vgl. § 69a Abs. 1 UrhG);

d) unter das Bankgeheimnis oder den Datenschutz oder eine ähnliche Geheimhaltungspflicht fallen oder von ähnlicher Natur wie die durch Bankgeheimnis oder Datenschutz geschützten Informationen sind

e) bei denen sich das Geheimhaltungsinteresse des offenbarenden Vertragspartners aus der Natur der Information ergibt. „Information“ meint sowohl die Daten als auch die mit den Daten versehenen Datenträger.

§ 1 Cooperation

(1) [Description of business relationship between the parties] (the “Cooperation”).

(2) With the present agreement, each contracting party receives protection for the information that has already been passed on and will still be passed on within the framework of this Cooperation.

§ 2 Confidential Information

(1) Confidential information within the meaning of this agreement is all information which

a) has been expressly designated in writing as confidential by a contractual partner;

b) belongs to information protected under §§ 17, 18 UWG, in particular knowhow;

c) is protected by industrial and other property rights, e.g. design material for software (cf. section 69a para. 1 UrhG);

d) is subject to banking secrecy or data protection or a similar obligation of secrecy or is of a similar nature as the information protected by banking secrecy or data protection

(e) where the disclosing party's interest in secrecy arises from the nature of the information. "Information" means both the data and the data carriers containing the data.

(2) Die Einbeziehung unter die vertraulichen Informationen entfällt oder endet, wenn

- a) die Information öffentlich bekannt ist;
- b) der offenbarende Vertragspartner schriftlich auf den Schutz verzichtet oder
- c) die Information dem empfangenden Vertragspartner auf anderem Wege als durch den offenbarenden Vertragspartner bekannt wurde und hierbei durch niemanden eine Geheimhaltungspflicht verletzt wurde.
Wer sich auf eine dieser Ausnahmen beruft, hat ihr Vorliegen zu beweisen.

§ 3 Gestattete Vorgänge

- (1) Der empfangende Vertragspartner darf die Information in der Weise und in dem Maße handhaben (auch kopieren), wie dies zur Durchführung der Zusammenarbeit zweckmäßig und üblich ist.
- (2) Der empfangende Vertragspartner darf die Information nur denjenigen seiner angestellten Mitarbeiter zur Verfügung stellen, die in die Zusammenarbeit einbezogen sind, und zwar in dem Maße, wie dies der Aufgabenstellung des Mitarbeiters im Rahmen der Zusammenarbeit entspricht. In diesem Maße darf er die Informationen auch seinen externen Beratern zur Verfügung stellen.

(2) Inclusion among the confidential information shall cease or terminate if

- a) the information is in the public domain
- b) the disclosing contracting party waives protection in writing; or
- c) the information became known to the receiving contracting party by means other than through the disclosing contracting party and no obligation of secrecy was breached by anyone in the process.
Whoever invokes one of these exceptions must prove its existence.

§ 3 Permitted Actions

- (1) The receiving contracting partner may handle (including copy) the information in the manner and to the extent that this is expedient and customary for the performance of the Cooperation.
- (2) The receiving contracting party may only make the information available to those of its employed staff who are involved in the Cooperation, and to the extent that this corresponds to the task of the employee within the framework of the Cooperation. To this extent, he may also make the information available to his external consultants.
- (3) The receiving contractual partner may transfer the information to third

(3) Der empfangende Vertragspartner darf die Information Dritten überlassen, wenn der übertragende Vertragspartner dem zuvor schriftlich zugestimmt hat. Wenn der Dritte ein mit dem empfangenden Vertragspartner nach § 15 AktG verbundenes Unternehmen ist und seine Kenntnisnahme für das gemeinsame Ziel (vgl. § 1) nützlich ist, darf der offenbarende Vertragspartner die Zustimmung nicht ohne nachvollziehbaren Grund verweigern.

(4) Der empfangende Vertragspartner darf die Information offenbaren, soweit er hierzu gesetzlich oder behördlich verpflichtet ist. Er beachtet hierbei § 4 Abs. 4

§ 4 Pflichten

(1) Der empfangende Vertragspartner schützt und sichert die vertraulichen Informationen mit der erforderlichen Sorgfalt, zumindest mit der Sorgfalt, mit welcher er eigene vergleichbare Informationen schützt. Informationen werden so verwahrt und gesichert, dass Missbrauch und unbefugte Kenntnisnahme ausgeschlossen sind.

(2) In Bezug auf Informationen nach § 2 Abs. 1 (d) kann der überlassende Vertragspartner verlangen, dass kenntnisnehmende Personen schriftlich zur Verschwiegenheit nach Maßgabe dieser Vereinbarung verpflichtet werden (vgl. § 53 BDSG) und dass dies dem überlassenden Vertragspartner im Voraus nachgewiesen wird.

(3) Der empfangende Vertragspartner unterrichtet den überlassenden Vertragspartner unverzüglich und schriftlich, wenn Kenntnis oder Verdacht von einer bevorstehenden oder stattgefundenen Verletzung der Geheimhaltungsinteressen des überlassenden Vertragspartners hat.

parties if the transferring contractual partner has agreed to this in writing in advance. If the third party is a company affiliated with the receiving contracting party pursuant to section 15 of the German Stock Corporation Act (AktG) and its knowledge is useful for the common objective (cf. section 1), the disclosing contracting party may not refuse consent without comprehensible reason.

(4) The receiving contracting party may disclose the information insofar as it is obliged to do so by law or by the authorities. In doing so, he/she shall observe § 4 para. 4

§ 4 Duties

(1) The receiving contracting party shall protect and secure the confidential information with the necessary care, at least with the care with which it protects its own comparable information. Information shall be stored and secured in such a way that misuse and unauthorised access are excluded.

(2) With regard to information according to § 2 para. 1 (d), the providing contracting party may demand that persons having knowledge are obliged in writing to maintain confidentiality in accordance with this agreement (cf. § 53 BDSG) and that this is proven to the providing contracting party in advance.

(3) The receiving contractual partner shall inform the assigning contractual partner immediately and in writing if it has knowledge or suspicion of an imminent or actual breach of the confidentiality interests of the assigning contractual partner.

Geschützt hierbei sind die Geheimhaltungsinteressen des überlassenden Vertragspartners gegenüber jedermann.

(4) Der empfangende Vertragspartner unterrichtet den überlassenden Vertragspartner unverzüglich und im Voraus von einer Weitergabe der Informationen nach § 3 Abs. 4.

§ 5 Unerlaubte Vorgänge

(1) Der empfangende Vertragspartner darf (soweit in § 3 oder in anderer Weise nichts anderes ausdrücklich schriftlich gestattet ist) Schutzrechte an den vertraulichen Informationen (insbesondere urheberrechtliche Befugnisse) nicht nutzen. Er darf auch sonst die Informationen (auch wenn sie nicht unter ein gesetzliches Schutzrecht fallen) in keiner Weise nutzen oder verwerten.

(2) Kein Vertragspartner darf angestellten Mitarbeitern des anderen Vertragspartners das Angebot machen, ihn während der Dauer dieser Vereinbarung und bis zum Ablauf zweier Kalenderjahre danach einzustellen (Abwerbeverbot). Das Abwerbeverbot verpflichtet auch verbundene Unternehmen des einen Vertragspartners und schützt auch im Sinne eines Vertrages zugunsten Dritter verbundene Unternehmen des anderen Vertragspartners in Bezug auf deren Mitarbeiter; die Vertragspartner stehen insofern hiermit für die Handlungen der mit ihnen jeweils verbundenen Unternehmen ein. Einem solchen Arbeitsvertrag stehen andere Angebote und Vereinbarungen gleich, aufgrund derer die Arbeitskraft des Mitarbeiters nicht mehr dem bislang anstellenden Unternehmen zugutekommt, sondern ganz oder teilweise dem Vertragspartner.

The confidentiality interests of the transferring contractual partner vis-à-vis everyone are protected in this respect.

(4) The receiving contracting party shall inform the transferring contracting party without delay and in advance of any disclosure of information pursuant to Article 3 (4).

§ 5 Unauthorised Actions

(1) The receiving contracting party may not (unless otherwise expressly provided in writing in § 3 or otherwise) use industrial property rights to the confidential information (in particular copyright rights). Nor may it otherwise use or exploit the information (even if it is not covered by a statutory property right) in any way.

(2) No contractual partner may make an offer to employed staff of the other contractual partner to employ him during the term of this agreement and until the expiry of two calendar years thereafter (non-solicitation). The non-solicitation clause also obliges affiliated companies of one contracting party and also protects, in the sense of a contract for the benefit of third parties, affiliated companies of the other contracting party with regard to their employees; the contracting parties are hereby liable for the actions of their respective affiliated companies. Other offers and agreements on the basis of which the employee's labour no longer benefits the previously employing enterprise but the contracting party in whole or in part are equivalent to such an employment contract.

§ 6 Vertragsstrafe

(1) Ein Vertragspartner, der Pflichten nach § 3, § 4 oder § 5 verletzt (Schuldner), hat dem anderen Vertragspartner (Gläubiger) für jeden Pflichtverstoß unter Verzicht auf die Einrede des Fortsetzungszusammenhangs eine Vertragsstrafe zu bezahlen. Die Vertragsstrafe beträgt für Verstöße gegen § 3, § 4, § 5 Abs. 1 zwischen EUR [•] und EUR [•]. Sie hat in diesem Rahmen billigem Ermessen zu entsprechen. Maßgeblich hierfür sind die Bedeutung der verletzten Pflicht, der Nachteil des Gläubigers (auch der immaterielle Nachteil) und der Grad der Pflichtverletzung und des Verschuldens des Schuldners. Einigen sich die Vertragspartner hierüber nicht, so entscheidet hierüber verbindlich als Schiedsgutachter ein vom Präsidenten des Oberlandesgerichtes [•] benannter Richter dieses Oberlandesgerichtes nach (auch nur schriftlicher) Anhörung der Vertragspartner.

(2) Für den Fall eines Verstoßes gegen § 5 Abs. 2 beträgt die Vertragsstrafe drei Bruttomonatsgehälter, wie der Mitarbeiter sie zuletzt zu bekommen hatte (bei variabler Vergütung bezogen auf die letzten 12 vollen Kalendermonate). Bei erfolgreicher Abwerbung beträgt die Vertragsstrafe das Doppelte.

§ 7 Dauer der Verpflichtung

Soweit nichts anderes vereinbart ist, gelten die Verpflichtungen aus der vorliegenden Vereinbarung auf Dauer.

§ 6 Contractual penalty

(1) A contracting party who breaches obligations under § 3, § 4 or § 5 (debtor) shall pay the other contracting party (creditor) a contractual penalty for each breach of obligation, waiving the defence of continuation of the contract. The contractual penalty for breaches of § 3, § 4, § 5 para. 1 shall be between EUR [•] and EUR [•] and shall be in accordance with reasonable discretion. The decisive factors are the significance of the breached obligation, the disadvantage to the creditor (including the immaterial disadvantage) and the degree of the breach of obligation and the fault of the debtor. If the parties to the contract do not agree on this, a judge of this Higher Regional Court appointed by the President of the Higher Regional Court [•] shall make a binding decision on this as an arbitrator after hearing the parties to the contract (even if only in writing).

(2) In the event of a breach of section 5 subsection 2, the contractual penalty shall amount to three gross monthly salaries as the employee last received them (in the case of variable remuneration based on the last 12 full calendar months). In the event of a successful enticement, the contractual penalty shall be twice that amount.

§ 7 Duration of the obligation

Unless otherwise agreed, the obligations under this Agreement shall be perpetual.

§ 8 Vertragsdauer

(1) Die Vereinbarung kann von jedem Vertragspartner jederzeit gekündigt werden, jedoch frühestens auf einen Zeitpunkt, zu welchem die in § 1 Abs. 1 genannte Zusammenarbeit endet.

(2) Die Vereinbarung endet in jedem Fall mit Ablauf eines vollen Kalenderquartals nach Ende der Zusammenarbeit.

§ 9 Schlussbestimmungen

(1) Die für Vorgänge bei der Durchführung der Vereinbarung angeordnete Schriftform wird auch durch Telefax und E-Mail eingehalten und auch, wenn die Festlegung in einem Protokoll über eine Besprechung zwischen den Vertragspartnern niedergelegt ist, das Protokoll allen Vertragspartnern vorliegt und binnen zwei Wochen kein schriftlicher Widerspruch erfolgt.

(2) [Schlussklauseln über anwendbares Recht, Gerichtsstand und Schriftform]

§ 8 Term of the agreement

(1) The agreement may be terminated by either contracting party at any time, but not earlier than the date on which the Cooperation referred to in Article 1(1) ends.

(2) The agreement shall end in any case at the end of a full calendar quarter after the end of the Cooperation.

§ 9 Final Provisions

(1) The written form prescribed for transactions in the execution of the agreement shall also be complied with by fax and e-mail and also if the stipulation is laid down in a record of a discussion between the contracting parties, the record is available to all contracting parties and no written objection is made within two weeks.

(2) [Final clauses on applicable law, place of jurisdiction and written form].

取引相手との秘密保持義務条項

§ 1 協力

(1) [当事者間取引関係の説明] (「本協力」又は「本合意」)

(2) 現在の合意の下で、各契約当事者は、本協力の枠組みの中で、すでに渡されている情報、並びに、引き続き渡される情報について、保護を享受する。

§ 2 機密情報

(1) 本合意内の「機密情報」とは、以下に該当するような、すべての情報である。

a) 契約当事者によって、機密として、書面で明示的に指定されている。

b) UWG § 17、18 で保護されている情報、特にノウハウに属している。

c) 産業財産権並びにその他財産権によって保護されている。例：ソフトウェアのデザイン素材

(UrhG 第 69a 条第 1 段落を参照)

d) 銀行秘密またはデータ保護の対象となっているか、同様の機密保持義務を生じさせるもの、又は、情報が、銀行秘密又はデータ保護で守られるために、銀行秘密によって保護される情報と同様の性質のもの。

e) 開示する当事者の機密性に関する利益が、情報の性質から生じるもの。

「情報」とは、データ及びデータを内蔵するデータキャリアをいう。

(2) 機密情報への内包は、次の場合に中止または終了する。

a) 情報はパブリックドメインにある。

b) 開示する契約当事者が、書面により保護を免除する。

c) 情報が、開示を受ける当事者に、開示する契約当事者から受けとる以外の手段で、秘密保持義務の違反の状況のない状態で、知られるようになった。

これらの例外の 1 つを主張する者は、誰でも、その存在を証明する必要がある。

§ 3 許可される行為

(1) 受領する契約当事者は、本協力の履行のために、効率的で、慣習的に行われうる方法および範囲で、情報を処理（コピーを含む）できる。

(2) 受領する当事者は、情報を利用できるようにするだけ

本協力に参与している、雇用されたスタッフにのみ、そしてこれが本協力の枠組内で職務を行う限りで、従業員に情報利用できるようにする。この限定内で、外部コンサルタントにも、情報を利用できるようにすることができる。

(3) 受領する当事者は、情報を与える当事者が、書面でこれに同意する場合、情報を第三者に転送することができる。第三者が、ドイツ株式法 (AktG) 第 15 条に基づき、受領当事者の関連会社の場合、及び、その知識が、共通の目的に有益である (§ 1 を参照) 場合には、開示する契約当事者は、理解しうる理由なく、同意を拒否することはできません。

(4) 受領当事者は、法律または規制当局による義務がある場合、情報を開示することができる。但し、受領当事者は、§ 4 第 4 段落を遵守しなければならない。

§ 4 義務

(1) 受領当事者は、必要な注意をもって、少なくとも、自己が同種の情報を保護するために払う注意と比較可能な程度に、機密情報を保護及び防御するものとする。情報は、誤用や無許可のアクセスが除外されるように、保護及び防御されるものとする。

(2) 提供する契約当事者は、§ 2 第 1 段落(d)の情報について、知識を有する者が、本合意 (BDSG § 53 を参照) に従って、機密性を維持することが義務付けられていること、並びに、これが、提供する契約当事者に証明されていることを、書面で要求することができる。

(3) 受領する契約当事者は、提供する契約当事者の機密性の利益への、差し迫った、若しくは、現実の違背についての認識又は疑いがある際には、直ちに、提供する契約当事者に、書面で通知するものとする。

(4) 受領締約国は、第 3 条(4)に基づく情報の開示に先立って、かつ、遅滞なく、提供する契約者に通知する。

§ 5 許されない行為

(1) 受領する当事者は、(§ 3 に基づく、又は、その他の書面で明記されていない限り) 機密情報に対する産業所有権を、特に著作権を、使用することはできない。また、(法定財産権の対象外であっても) 情報を使用又は搾取することはできない。

(2) 契約当事者は、他の契約当事者の雇用されたスタッフに、本契約期間及びその後 2 暦年の間、雇用するために、雇用の申し出をしてはならない(非勧誘)。非勧誘条項は、契約当事者の関連会社をも同様に義務づけ、更に、第三者の利益のための契約の意味で、相手方契約当事者の関連会社の従業員に関しても、保護の対象とする。契約当事者は、これにより、それぞれの関連会社の行動に対して責任を負う。契約又は申出のうち、従業員の労働が、全体または一部で、以前の雇用主である契約当事者に利益をもたらさなくなり、他の契約当事者に利益となるものは、勧誘の雇用契約に相当する。

§ 6 契約上の罰金

(1) § 3、§ 4、又は § 5 に基づく義務に違反する契約当事者(債務者)は、契約継続の抗弁を放棄し、他の契約当事者(債権者)に、それぞれの義務違反に、契約上の罰金を支払う。§ 3、§ 4、及び、§ 5 第 1 項の義務違反に対する契約上の罰金は、EUR [・] と EUR [・] の間の額であり、合理的な裁量に従う。決定的な要因は、違反された義務の重要性、債権者への不利益(重要でない不利益を含む)、違反の程度、及び債務者の過失である。もしも、契約当事者間に同意が得られない場合、当事者双方の主張立証を聞いた後(書面のみであっても)、当該地域の高等裁判所裁判長によって任命された高等地方裁判所の裁判官を仲裁人とした仲裁により、拘束力のある決定で解決されることに同意する。

(2) § 5 第 2 項の違反が発生した場合、契約上の罰金は、従業員が最後に受取した月給総額の 3 倍になる。(変動報酬の場合、過去 12 全暦月に基づく)。勧誘が成功した場合、契約上の罰金は、この 2 倍の額になる。

§ 7 義務の存続期間

別段の合意がない限り、本契約に基づく義務は永続的である。

§ 8 本契約の期間

(1) 本契約は、いつでも、どちらかの契約当事者により終了する場合がある。しかし、第1条(1)で言及されている、本協力日終了日より前でない。

(2) 本契約は、いかなる場合でも、本協力の終了後、完全な暦四半期で終了するものとする。

§9 終局的規定

(1) 本契約締結時の取引について定められた書面は、ファックスと電子メールでも交わされるものとする。もし、本契約の定めが、契約当事者の協議の記録に記載された場合、すべての契約当事者がその記録を利用でき、2週間以内に書面による異議申立てが行われないことを要する。

(2) [準拠法、管轄地、及び、本契約書面の方式についての、最終的な条項]。

5 来訪者受付表

Annex 5 – Visitor list for a business site

Visitor Name	Visitor Address	Host	Time of Arrival	Time of Departure	Visitor Information Approved by:

* * *

(参考和訳) 来訪者受付表

事業所の訪問客リスト

訪問客名	訪問客住所	ホスト	到着時刻	出発時刻	訪問客情報許可者

第3章 英国における参考書式

1 就業規則における秘密保護関連規定の例

Staff handbook

6. Introduction

6.1 [GENERAL DETAILS ABOUT THE EMPLOYER AND ITS BUSINESS.]

6.2 We are an equal opportunities employer and do not discriminate on the grounds of gender, sexual orientation, marital or civil partner status, pregnancy or maternity, gender reassignment, race, colour, nationality, ethnic or national origin, religion or belief, disability or age.

7. Using the Staff Handbook

7.1 This Staff Handbook sets out the main policies and procedures that you will need to be aware of while working for us. You should familiarise yourself with it and comply with it at all times. Any questions you may have with regard to its contents or what you have to do to comply with it should be referred to the Human Resources Department.

7.2 The policies and procedures set out in this handbook apply to all employees unless otherwise indicated. They therefore apply to managers, officers, directors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, casual and agency staff and volunteers (collectively referred to as **staff** in this handbook). They do **not** form part of the terms of your contract with us, which are provided to you separately.

8. Responsibility for the Staff Handbook

8.1 The HR Manager has overall responsibility for this Staff Handbook and for ensuring that its policies and procedures comply with our legal obligations.

8.2 The Staff Handbook is reviewed regularly to ensure that its provisions continue to meet our legal obligations and reflect best practice.

8.3 Everyone should ensure that they take the time to read and understand the content of this handbook and act in accordance with its aims and objectives. Managers must ensure all staff understand the standards of behaviour expected of them and to take action when behaviour falls below those requirements.

9. Personal data

9.1 Whenever we process personal data about you in connection with our policies, we will process it in accordance with our Data Protection Policy. We will only process your personal data if we have

a lawful basis for doing so. We will notify you of the purpose or purposes for which we use it. Please see the intranet for further information.

10. Emergency contact details

- 10.1 The Human Resources Department is responsible for maintaining up-to-date details of your home address and the emergency contact telephone numbers of the person or persons you would like us to contact in the event of an emergency, for example if you have an accident. This information will be requested by the Human Resources Department when you start work and you will periodically be asked to confirm that these are up to date]. This information is held in confidence and will only be used when needed.

Schedule 1 Dress code

1. About this policy

- 1.1 We encourage everyone to maintain an appropriate standard of dress and personal appearance at work. The purpose of our dress code is to establish basic guidelines on appropriate clothing and appearance at our workplace, so that we:
 - (a) promote a positive and professional image;
 - (b) respect the needs of men and women from all cultures and religions;
 - (c) make any adjustments that may be needed because of disability;
 - (d) take account of health and safety requirements; and
 - (e) help staff and managers decide what clothing it is appropriate to wear to work.
- 1.2 Managers are responsible for ensuring that this dress code is observed and that a common sense approach is taken to any issues that may arise. Any enquiries regarding the operation of our dress code (including whether an article of clothing is suitable to wear to work) should be made to your line manager or the Human Resources Department.
- 1.3 Failure to comply with the dress code may result in action under our Disciplinary Procedure.
- 1.4 We will review our dress code periodically to ensure that it reflects appropriate standards and continues to meet our needs.
- 1.5 This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. Appearance

- 2.1 While working for us you represent us with customers and the public. Your appearance contributes to our reputation and the development of our business.
- 2.2 It is important that you appear clean and smart at all times when at work, particularly when you may be in contact with clients, other business contacts or the general public.
- 2.3 [Different departments may have specific clothing requirements, for example, because their work is customer-facing or raises particular health and safety concerns. It is important that you dress in a manner appropriate to your working environment and the type of work you do.]
- 2.4 All employees in customer facing roles should wear smart business attire.

- 2.5 Employees in certain roles may be asked to cover up visible tattoos or to remove or cover up visible body piercings.
- 2.6 Footwear must be safe and clean and take account of health and safety considerations. Trainers, stilettos and flip-flops are not acceptable.
- 2.7 Where we provide safety clothing and equipment, including protective footwear, it should be worn or used as appropriate and directed.

3. Religious and cultural dress

- 3.1 You may wear appropriate religious and cultural dress (including clerical collars, head scarves, skullcaps and turbans) unless it creates a health and safety risk to you or any other person or otherwise breaches this policy.
- 3.2 Where necessary the Human Resources Department can give further information and guidance on cultural and religious dress in the workplace.
- 3.3 Priority is at all times given to health and safety requirements. Where necessary, advice will be taken from the Health and Safety Officer.

Schedule 2 Expenses policy

1. About this policy

- 1.1 This policy deals with claims for reimbursement of expenses, including travel, accommodation and hospitality.
- 1.2 This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. Reimbursement of expenses

3. Travel expenses

4. Accommodation and other overnight expenses

5. Entertaining [clients OR customers]

Schedule 3 Equal opportunities policy

Schedule 4 Anti-harassment and bullying policy

Schedule 5 Anti-corruption and bribery policy

Schedule 6 Whistleblowing policy

1. Confidentiality

- 1.1 We hope that staff will feel able to voice whistleblowing concerns openly under this policy. Completely anonymous disclosures are difficult to investigate. If you want to raise your concern confidentially, we will make every effort to keep your identity secret and only reveal it where necessary to those involved in investigating your concern.

2. External disclosures

- 2.1 The aim of this policy is to provide an internal mechanism for reporting, investigating and remedying any wrongdoing in the workplace. In most cases you should not find it necessary to alert anyone externally.
- 2.2 The law recognises that in some circumstances it may be appropriate for you to report your concerns to an external body such as a regulator. We strongly encourage you to seek advice before reporting a concern to anyone external. Protect operates a confidential helpline. Their contact details are at the end of this policy.

3. Protection and support for whistleblowers

- 3.1 We aim to encourage openness and will support whistleblowers who raise genuine concerns under this policy, even if they turn out to be mistaken.
- 3.2 Whistleblowers must not suffer any detrimental treatment as a result of raising a genuine concern. If you believe that you have suffered any such treatment, you should inform [the Whistleblowing Officer **OR** [POSITION]] immediately. [If the matter is not remedied you should raise it formally using our Grievance Procedure.]
- 3.3 You must not threaten or retaliate against whistleblowers in any way. If you are involved in such conduct you may be subject to disciplinary action. [In some cases the whistleblower could have a right to sue you personally for compensation in an employment tribunal.]
- 3.4 However, if we conclude that a whistleblower has made false allegations maliciously, the whistleblower may be subject to disciplinary action.
- 3.5 Protect operates a confidential helpline. Their contact details are at the end of this policy.

4. **Contacts**

Whistleblowing Officer	[NAME] [TELEPHONE] [E-MAIL]
[Managing Director [OR OTHER TRUSTED INDIVIDUAL]]	[NAME] [TELEPHONE] [E-MAIL]
Protect (Independent whistleblowing charity)	Helpline: 0203 117 2520 E-mail: Website:

Schedule 7 Holidays policy

Schedule 8 Disciplinary and capability procedure

Schedule 9 Grievance procedure

Schedule 10 Sickness absence policy

Schedule 11 Time off for antenatal appointments policy

Schedule 12 Time off for adoption appointments policy

Schedule 13 Maternity policy

Schedule 14 Adoption policy

Schedule 15 Paternity policy

Schedule 16 Shared parental leave (birth) policy

Schedule 17 Shared parental leave (adoption) policy

Schedule 18 Parental leave policy

Schedule 19 Time off for dependants policy

Schedule 20 Compassionate leave policy

Schedule 21 Parental bereavement leave policy

Schedule 22 Flexible working policy

1. About this policy

- 1.1 This flexible working policy gives eligible employees an opportunity to request a change to their working pattern.
- 1.2 We will deal with flexible working requests in a reasonable manner and within a reasonable time. In any event the time between making a request and notifying you of a final decision (including the outcome of any appeal) will be less than three months unless we have agreed a longer period with you.
- 1.3 This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. Eligibility

- 2.1 To be eligible to make a flexible working request, you must:
 - (a) be an employee;
 - (b) have worked for us continuously for at least 26 weeks at the date your request is made; and
 - (c) not have made a flexible working request during the last 12 months (even if you withdrew that request).

3. What is a flexible working request?

- 3.1 A flexible working request under this policy means a request to do any or all of the following:
 - (a) to reduce or vary your working hours;
 - (b) to reduce or vary the days you work;
 - (c) to work from a different location (for example, from home).

4. Making a flexible working request

- 4.1 Your flexible working request should be submitted to [us **OR** [POSITION]] in writing and dated. It should:
 - (a) state that it is a flexible working request;
 - (b) explain the change being requested and propose a start date;
 - (c) identify the impact the change would have on the business and how that might be dealt with; and
 - (d) state whether you have made any previous flexible working requests.

5. Meeting

- 5.1 We will arrange a meeting at a convenient time and place to discuss your request. You may be accompanied at the meeting by a colleague of your choice. They will be entitled to speak and confer privately with you, but may not answer questions on your behalf.
- 5.2 We may decide to grant your request in full without a meeting, in which case we will write to you with our decision.

6. Decision

- 6.1 We will inform you in writing of our decision as soon as possible after the meeting.
- 6.2 If your request is accepted, we will write to you with details of the new working arrangements and the date on which they will commence. You will be asked to sign and return a copy of the letter.
- 6.3 If we cannot immediately accept your request we may require you to undertake a trial period before reaching a final decision on your request.
- 6.4 Unless otherwise agreed, changes to your terms of employment will be permanent.
- 6.5 We may reject your request for one or more of the following business reasons:
 - (a) the burden of additional costs;
 - (b) detrimental effect on ability to meet customer demand;
 - (c) inability to reorganise work among existing staff;
 - (d) inability to recruit additional staff;
 - (e) detrimental impact on quality;
 - (f) detrimental impact on performance;
 - (g) insufficiency of work during the periods that you propose to work; or
 - (h) planned changes.
- 6.6 If we are unable to agree to your request, we will write to tell you which of those reasons applies in your case. We will also set out the appeal procedure.

7. Appeal

- 7.1 You may appeal in writing within 14 days of receiving our written decision. [This includes a decision following a trial period.]

- 7.2 Your appeal must be dated and must set out the grounds on which you are appealing.
- 7.3 We will hold a meeting with you to discuss your appeal. You may bring a colleague to the meeting.
- 7.4 We will tell you in writing of our final decision as soon as possible after the appeal meeting, including reasons. There is no further right of appeal.

Schedule 23 Time off for public duties policy

Schedule 24 Health and safety policy

Schedule 25 [Privacy Standard OR Data Protection Policy]

Schedule 26 IT and communications systems policy

1. About this policy

- 1.1 Our IT and communications systems are intended to promote effective communication and working practices. This policy outlines the standards you must observe when using these systems, when we will monitor their use, and the action we will take if you breach these standards.
- 1.2 [POSITION] has overall responsibility for this policy, including keeping it under review.
- 1.3 Breach of this policy may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.
- 1.4 This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. Equipment security and passwords

- 2.1 You are responsible for the security of the equipment allocated to or used by you, and you must not allow it to be used by anyone other than in accordance with this policy. You should use passwords on all IT equipment, particularly items that you take out of the office. You should keep your passwords confidential and change them regularly.
- 2.2 You may use the equipment allocated to you only to serve our business goals. You may not use the equipment for anything that does not support or augment our business.
- 2.3 You must only log on to our systems using your own username and password. You must not use another person's username and password or allow anyone else to log on using your username and password.
- 2.4 If you are away from your desk you should log out or lock your computer. You must log out and shut down your computer at the end of each working day.

3. Systems and data security

- 3.1 You should not delete, destroy or modify existing systems, programs, information or data (except specifically authorised in the proper performance of your duties).
- 3.2 You must obtain a permission from your supervisor and our security manager for accessing, obtaining, retaining, transferring, copying, disclosing, communicating, or altering technical and operational information about existing our computer systems, networks, and IT infrastructures.

- 3.3 You must obtain a permission from your supervisor and our data security manager for transferring, copying, uploading, disclosing, communicating, or altering information and data that you have access to in connection with performance of your work and is not shared with outside people or other staff who are not given access to such information and data by our security manager.
- 3.4 You must not download or install software from external sources without authorisation from [POSITION]. Downloading unauthorised software may interfere with our systems and may introduce viruses or other malware.
- 3.5 You must not attach any device or equipment including mobile phones, tablet computers or USB storage devices to our systems without authorisation from [POSITION].
- 3.6 We monitor all e-mails passing through our system for viruses. You should exercise particular caution when opening unsolicited e-mails from unknown sources. If an e-mail looks suspicious do not reply to it, open any attachments or click any links in it.
- 3.7 Inform [POSITION] immediately if you suspect your computer may have a virus or malware.
- 3.8 Upon termination of your employment, you must return all the equipment allocated to or used by you as they should be.

4. E-mail

- 4.1 Adopt a professional tone and observe appropriate etiquette when communicating with third parties by e-mail. [You should also include our standard e-mail signature and disclaimer.]
- 4.2 Remember that e-mails can be used in legal proceedings and that even deleted e-mails may remain on the system and be capable of being retrieved.
- 4.3 You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate e-mails.
- 4.4 You should not:
 - (a) send or forward private e-mails at work which you would not want a third party to read;
 - (b) send or forward chain mail, junk mail, cartoons, jokes or gossip;
 - (c) contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to others who do not have a real need to receive them; or
 - (d) send messages from another person's e-mail address (unless authorised) or under an assumed name.

- 4.5 Do not use your own personal e-mail account to send or receive e-mail for the purposes of our business. Only use the e-mail account we have provided for you.
- 4.6 [We do not permit access to web-based personal e-mail such as Gmail or Hotmail on our computer systems at any time due to additional security risks.]

5. Using the internet

- 5.1 Internet access is provided solely for business purposes.
- 5.2 You should not access any web page or download any image or other file from the internet which could be regarded as illegal, offensive, in bad taste or immoral. Even web content that is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.
- 5.3 We may block or restrict access to some websites at our discretion.

6. Personal use of our systems

7. Monitoring

- 7.1 Our systems enable us to monitor telephone, e-mail, voicemail, internet and other communications. For business reasons, and in order to carry out legal obligations in our role as an employer, your use of our systems including the telephone and computer systems (including any personal use) may be continually monitored by automated software or otherwise.
- 7.2 We reserve the right to retrieve the contents of e-mail messages or check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, including for the following purposes (this list is not exhaustive):
 - (a) to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy;
 - (b) to find lost messages or to retrieve messages lost due to computer failure;
 - (c) to assist in the investigation of alleged wrongdoing; or
 - (d) to comply with any legal obligation.

8. Prohibited use of our systems

- 8.1 Misuse or excessive personal use of our telephone or e-mail system or inappropriate internet use will be dealt with under our Disciplinary Procedure. Misuse of the internet can in some cases be a criminal offence.
- 8.2 Creating, viewing, accessing, transmitting or downloading any of the following material will usually amount to gross misconduct (this list is not exhaustive):
- (a) pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);
 - (b) offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our clients;
 - (c) a false and defamatory statement about any person or organisation;
 - (d) material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Equal Opportunities Policy or our Anti-harassment and Bullying Policy);
 - (e) confidential information about us or any of our staff or clients (except as authorised in the proper performance of your duties);
 - (f) unauthorised software;
 - (g) any other statement which is likely to create any criminal or civil liability (for you or us);
or
 - (h) music or video files or other material in breach of copyright.

Schedule 27 Social media policy

1. About this policy

- 1.1 This policy is in place to minimise the risks to our business through use of social media.
- 1.2 This policy deals with the use of all forms of social media, including Facebook, LinkedIn, Twitter, Google+, Wikipedia [, Whisper] [, Instagram] [, Tumblr] and all other social networking sites, internet postings and blogs. It applies to use of social media for business purposes as well as personal use that may affect our business in any way.
- 1.3 This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. Personal use of social media

- 2.1 [Personal use of social media is never permitted during working hours or by means of our computers, networks and other IT resources and communications systems.

OR

Occasional personal use of social media during working hours is permitted so long as it does not involve unprofessional or inappropriate content, does not interfere with your employment responsibilities or productivity and complies with this policy.]

3. Prohibited use

- 3.1 You must avoid making any social media communications that could damage our business interests or reputation, even indirectly.
- 3.2 You must not use social media to defame or disparage us, our staff or any third party; to harass, bully or unlawfully discriminate against staff or third parties; to make false or misleading statements; or to impersonate colleagues or third parties.
- 3.3 You must not express opinions on our behalf via social media, unless expressly authorised to do so by your manager. You may be required to undergo training in order to obtain such authorisation.
- 3.4 You must not post comments about sensitive business-related topics, such as our performance, or do anything to jeopardise our trade secrets, confidential information and intellectual property. You must not include our logos or other trademarks in any social media posting or in your profile on any social media.

- 3.5 [You are not permitted to add business contacts made during the course of your employment to personal social networking accounts.

OR

The contact details of business contacts made during the course of your employment are our confidential information. On termination of employment you must provide us with a copy of all such information, delete all such information from your personal social networking accounts and destroy any further copies of such information that you may have.]

- 3.6 Any misuse of social media should be reported to [POSITION].

4. Guidelines for responsible use of social media

- 4.1 You should make it clear in social media postings, or in your personal profile, that you are speaking on your own behalf. Write in the first person and use a personal e-mail address.
- 4.2 Be respectful to others when making any statement on social media and be aware that you are personally responsible for all communications which will be published on the internet for anyone to see.
- 4.3 If you disclose your affiliation with us on your profile or in any social media postings, you must state that your views do not represent those of your employer (unless you have been authorised to speak on our behalf as set out in paragraph 3.3). You should also ensure that your profile and any content you post are consistent with the professional image you present to clients and colleagues.
- 4.4 If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from posting it until you have discussed it with your manager.
- 4.5 If you see social media content that disparages or reflects poorly on us, you should contact [your manager **OR** [DEPARTMENT]].

5. Breach of this policy

- 5.1 Breach of this policy may result in disciplinary action up to and including dismissal. [Any member of staff suspected of committing a breach of this policy will be required to co-operate with our investigation.
- 5.2 You may be required to remove any social media content that we consider to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

就業規則

1. 初めに

1.1 [雇用主とその事業に関する一般的記載]

- 1.2 当社は、機会均等を目指す雇用主であり、性別、性的指向、婚姻若しくは市民権のパートナーの地位、妊娠若しくは出産、性別の再割当て、人種、肌の色、国籍、民族若しくは出身国、宗教若しくは信念、障害、又は年齢を理由に、差別しない。

2. 就業規則の使用について

- 2.1 本就業規則は、あなたが、当社のために働いている間、あなたが知っておく必要がある、主要な方針や手続きを示す。あなたは、これに精通し、常に、従わないとしない。この内容、あるいは、これを遵守するためにあなたがしなければならないことに関して、あなたが持つ疑問については、人事部に照会されるべきである。
- 2.2 このハンドブックに記載されている方針及び手順は、特に明記されていない限り、すべての従業員に適用される。したがって、これらは、マネージャー、役員、取締役、従業員、コンサルタント、請負業者、研修生、在宅勤務者、パートタイム、並びに、有期労働者、臨時スタッフ、並びに、代理店のスタッフ、及び、ボランティア（このハンドブックでは、まとめて「従業員」と呼ぶ。）に適用される。これらは、別途提供される、当社との契約条件の一部を構成するものではない。

3. 就業規則への責任

- 3.1 人事部長は、この従業員ハンドブックに対して、全体的な責任を負い、その方針及び手順が、当社の法的義務に準拠していることを確認する。
- 3.2 スタッフハンドブックは定期的に見直され、その規定が、引き続き当社の法的義務を果たし、ベストプラクティスを反映しているか、確認される。
- 3.3 各従業員は、時間をかけ、このハンドブックの内容を読んで理解し、その趣旨と目的に従って行動する。管理者は、全従業員が、彼らに期待される行動の基準を理解し、行動がその要件を下回ったときに、確実に対処しなければならない。

4. 個人情報

- 4.1 当社の方針に関連して、あなたの個人データを処理する場合は、常に、データ保護ポリシーに従って処理される。あなたの個人データは、合法的な理由がある場合にのみ、処

理される。当社は、あなたにデータの使用目的を通知する。詳細については、イントラネットのプライバシー通知を参照するものとする。

5. 緊急連絡先

人事部は、自宅の住所、及び、事故などの緊急時に、当社に連絡を取らせたい緊急連絡先の電話番号、の最新情報の詳細を維持する責任がある。これらの情報は、あなたが職務を開始するときに、人事部から要求され、定期的に、これらが最新であることを確認するように求められる]。この情報は機密情報として保持され、必要な場合にのみ使用される。

Schedule 1 ドレスコード

1. この方針について

- 1.1 私たちは、すべての者が、職場における、適切な服装と個人的な外見の基準を、維持することを勧奨する。ドレスコードの目的は、職場での適切な服装と外見に関する、基本的なガイドラインを確立することにある、そして：
 - (a) ポジティブでプロフェッショナルなイメージを促進する。
 - (b) すべての文化と宗教の、男性と女性のニーズを尊重する。
 - (c) 障害のために必要となる可能性のある調整を行う。
 - (d) 健康と安全の要求を考慮に入れる。
 - (e) スタッフと管理者が、仕事に着るのに適切な服を、決める助けとなる。
- 1.2 管理者は、このドレスコードが遵守され、発生する可能性のある問題に対して、常識的なアプローチが取られるようにする責任がある。ドレスコードの運用に関する問い合わせ（衣服が仕事に適しているかどうかを含む）は、ラインマネージャーまたは人事部に連絡すること。
- 1.3 ドレスコードに従わない場合は、懲戒手続きに基づく措置が取られる可能性がある。
- 1.4 ドレスコードは、定期的に見直され、適切な基準を反映し、ニーズを依然として満たしているかが確認される。
- 1.5 この方針は、従業員の雇用契約の一部を構成するものではなく、いつでも修正することができる。

2. 外見

- 2.1 私たちのために働いている間、あなたは、顧客や一般の人々に、私たちを代表する。あなたの外見は、私たちの評判と、私たちのビジネスの発展に、貢献する。
- 2.2 工作中、特に、顧客、他のビジネス上の連絡先、または、一般の人々と接触している可能性があるとき、常に、清潔で、賢明に見えることが重要となる。
- 2.3 [たとえば、部門ごとに、特定の衣服の要求がある場合がある。たとえば、仕事は顧客と接するため、または、特定の健康と安全上の問題を引き起こしうるためであり、作業環境や、作業の種類に適した服装をする、ことが重要である。]

- 2.4 顧客対応の役割を担う従業員は、全て、賢実なビジネス服を着る必要がある。
- 2.5 特定の役割の従業員は、目に見える入れ墨を隠すか、目に見えるボディピアスを取り除くか、隠すように、求められる場合がある。
- 2.6 履物は、安全で清潔でなければならない、健康と安全のための考慮事項を、検討しなければならない。トレーナー、ハイヒール、フリップフロップは、着用できない。
- 2.7 保護靴を含む、安全服および装備を提供する場合は、必要に応じて、若しくは、指示に従って、着用、又は、使用する必要がある。
- 3. **宗教的、文化的衣服**
 - 3.1 あなたや他者への健康、安全上のリスクを生んだり、他の規則に違反しない限り、あなたは、適切な、宗教的、並びに、文化的な衣服（僧の襟、頭巾、帽子、ターバンを含む）を身につけることができる。.
 - 3.2 必要な場合、人事部は、職場の文化的、及び、宗教的服装について、更に情報やガイダンスを提供する。
 - 3.3 健康、安全の要求が常に優先される。必要な場合、健康安全役員からアドバイスを得られる。

Schedule 2 内部告発方針

1. 機密性

- 1.1 この方針の下で、スタッフが、内部者の不正の懸念を公然と表明できるようになることを願う。完全に匿名の開示を、調査することは困難である。あなたが、秘密裏に懸念を提起したい場合、私たちは、あなたの身元を秘密に保つために、あらゆる努力をし、あなたの懸念の調査に関与する人々に必要な場合にのみ、それを明らかにする。

2. 外部への開示

- 2.1 このポリシーの目的は、職場での不正行為を報告、調査及び是正するための内部メカニズムを提供することである。ほとんどの場合、外部の者に警告する必要はない。
- 2.2 法律は、状況によっては、規制当局などの外部機関に、懸念を報告することが適切な場合があることを認める。外部者に懸念を報告する前に、アドバイスを求めることを強く勧める。[機関の名前] は、機密のヘルプラインを運営している。その連絡先の詳細は、このポリシーの最後に記載されている。

3. 内部告発者の保護と支持

- 3.1 当社は、開放性を励まし、この方針下に真摯に懸念を表明する内部告発者に、たとえ間違っていたとしても、サポートを与える。
- 3.2 内部告発者は、真摯な懸念を表明した結果として、不当な扱いを受けてはならない。そのような扱いを受けたと思われる場合は、直ちに[内部告発責任者[]に]申告する必要がある。[問題が解決されない場合は、異議申立手続を使用して、正式に問題提起する必要がある。]
- 3.3 内部告発者に対して、いかなる方法でも、脅迫したり、報復したりしてはならない。あなたが、そのような行為に関与している場合、あなたは懲戒処分の対象となる可能性がある。[場合によっては、内部告発者は、雇用審判所で、損害賠償請求のために、あなたを個人的に訴えることがある。]
- 3.4 しかし、もし、当社で、内部告発者が、虚偽の主張を悪意で行ったと認めた場合には、内部告発者は、懲戒処分の対象となりうる。
- 3.5 [機関の名前]は、機密のヘルプラインを運営している。この方針の最後に、その連絡先がある。

4. 連絡先

内部告発役員	[名前] [電話] [E-MAIL]
[業務執行員 [又は、他の信用される個人]]	[名前] [電話] [E-MAIL]
[機関の名称／Protect] (独立した公益機関)	Helpline: 0203 117 2520 E-mail: Website:

Schedule 3 IT 及び通信システム方針

1. この方針について

- 1.1 当社の IT 及び通信システムは、効果的なコミュニケーション及び作業慣行を促進することを目的としている。この方針は、これらのシステムを使用するときに遵守しなければならない基準、それらの使用を監視する時期、及びこれらの基準に違反した場合に実行する行動の概要を示している。
- 1.2 []は、この方針の見直しの継続を含め、この方針に対して、全体的に責任を負う。
- 1.3 この方針の違反は、懲戒手続で対応される可能性があり、深刻な場合には、即時解雇につながる重大な逸脱行為として扱われる可能性がある。
- 1.4 この方針は、従業員の雇用契約の一部を形成するものではなく、当社において、随時改変することができる。

2. 機器の安全性及びパスワード

- 2.1 あなたは、あなたに割り当てられた、または、あなたが使用する機器の安全性に責任を負い、この方針に服する者以外の者による使用を許可してはならない。すべての IT 機器、特に、オフィスから持ち出す品目には、パスワードを使用しなければならない。パスワードは、内密にし、定期的に変更する必要がある。
- 2.2 割り当てられた機器は、当社のビジネス目標を達成するためにのみ、使用できる。当社の事業の支持または発展以外の目的で、機器を使用してはならない。
- 2.3 自分のユーザー名及びパスワードを使用してのみ、システムにログオンしなければならない。他人のユーザー名及びパスワードを使用したり、他人に、自分のユーザー名及びパスワードを使用してログオンさせたりしてはならない。
- 2.4 端末から離れている場合は、ログアウトするか、コンピューターをロックする。終業時には、ログアウトして、コンピューターをシャットダウンしなければならない。

3. システム及びデータの安全性

- 3.1 既存のシステム、プログラム、情報若しくはデータを、削除、破棄、又は変更してはならない（職務の適切な遂行において、特別に許可されている場合を除く。）。

- 3.2 既存のコンピューターシステム、ネットワーク並びに IT 基盤に関する技術情報及び運用情報にアクセス、取得、保持、転送、コピー、開示、通信、又は変更するには、上司及びセキュリティマネージャーから、許可を得なければならない。
- 3.3 業務の遂行に関連してアクセスでき、外部者、並びに、当社のセキュリティマネージャーから、そのような情報やデータへのアクセスを許可されていないスタッフと、共有されていない情報及びデータを、転送、コピー、アップロード、開示、伝達、又は変更するには、上司及びデータセキュリティマネージャーから、許可を得る必要がある。
- 3.4 []の許可なしに、外部ソースからソフトウェアをダウンロード、又はインストールしてはならない。許可されていないソフトウェアをダウンロードすると、システムに影響を与え、ウイルスやその他のマルウェアを導入する可能性がある。
- 3.5 []の許可なしに、携帯電話、タブレットコンピューター、USB ストレージデバイス等のデバイスを、システムに接続してはならない。
- 3.6 システムを通過する、すべての電子メールを、ウイルス感染について監視する。送信元不明の迷惑メールを開く場合は、特に注意すること。電子メールが疑わしいと考える場合には、返信、添付ファイル開封、及びその中のリンクをクリック、をいずれもしてはならない。
- 3.7 コンピュータにウイルスまたはマルウェアが含まれている可能性がある場合は、直ちに []に通知する。
- 3.8 雇用終了時に、割り当てられた、または使用された、すべての機器を本来あるべき状態で返却する必要がある。

4. E-mail

- 4.1 電子メールで第三者とコミュニケーションをとるときは、業務上の口調を採用し、適切なエチケットに沿ったものとする。[標準の電子メール署名と、免責事項も含める必要がある。]
- 4.2 電子メールは、法的手続で使用でき、削除された電子メールもシステムに残り、取得できる可能性があることに注意する。
- 4.3 虐待的、わいせつな、差別的、人種差別的、嫌がらせの、侮蔑的、中傷的、性的表現の、又は、その他不適切な電子メールを送信してはならない。
- 4.4 以下は禁止される：
 - (a) 第三者に読まれたくない、職場の内密な電子メールを送信、又は転送する。

(b) チェーンメール、ジャンクメール、漫画、ジョーク、ゴシップを、送信、又は転送する。

(c) 些細なメッセージを送信したり、実際に受信する必要のない他者に、電子メールを不必要にコピー、又は転送したりすることで、システム混雑に加担する。

(d) 他者の電子メールアドレス（許可されていない場合）又は仮名で、メッセージを送信する。

4.5 当社の業務目的で電子メールを送受信するために、あなた自身の個人的な電子メールアドレスを使用してはならない。提供された電子メールアドレスのみを使用しなければならない。

4.6 [追加のセキュリティリスクのため、Gmail や Hotmail などの Web ベースの個人用電子メールへのアクセスをコンピューターシステムでいつでも許可していない。]

5. インターネットの使用

5.1 インターネットへのアクセスは、業務目的のみに付与されている。

5.2 違法、攻撃的、悪趣味、又は不道德と見なされる可能性のある、Web ページにアクセスしたり、インターネットから画像やその他のファイルをダウンロードしたりしてはならない。英国内で合法である Web コンテンツであっても、この禁止事項に該当する程度に悪趣味である可能性が存在する。原則として、（ページを表示することを意図しているかどうかにかかわらず）誰かがページのコンテンツに当惑する可能性がある場合、又は、当社のソフトウェアが、ページまたはファイルにアクセスしたという事実が公開された場合、問題となる可能性がある場合、当該表示が、この方針違反となる。

5.3 当社の裁量で、いくつかのウェブサイトブロックしたり、アクセス制限したりすることがある。

6. 当社システムの個人使用

[個人メールのチェックなど、許されるものがある場合には、許可内容を記載]

7. 監視

7.1 当社のシステムは、電話、電子メール、ボイスメール、インターネット、その他の通信を監視することができる。業務上の理由から、また、雇用主としての当社の役割から、法的義務を遂行するために、電話及びコンピューターシステムを含む、当社のシステムの使用（個人的な使用を含む。）は、自動ソフトウェア又はその他の方法で、継続的に監視される場合がある。

- 7.2 当社は、以下の目的を含め、業務上の利益のために合理的に必要な場合、電子メールメッセージの内容を取得したり、インターネットの使用状況（アクセスしたページや行われた検索を含む。）を確認したりする権利を留保する（このリストは網羅的ではない。）。
- (a) 電子メールシステムまたはインターネットの使用が合法であり、このポリシーに準拠しているかどうかを監視するため。
- (b) 失われたメッセージを検索するため、又は、コンピューターの障害のために失われたメッセージを取得するため。
- (c) 申し立てられた不正行為の調査を支援するため。
- (d) 法的義務を遵守するため。
8. **当社システムの禁止される使用**
- 8.1 当社の電話又は電子メールシステムの誤用、過度の個人的使用、若しくは、不適切なインターネットの使用は、懲戒手続で対応する。インターネットの誤用は、場合によっては、犯罪となる可能性がある。
- 8.2 次の資料の作成、表示、アクセス、送信、又はダウンロードは、通常、重大な逸脱行為となる（このリストは網羅的ではない）。
- (a) ポルノ素材（つまり、性的に露骨または興奮する性質の文章、写真、映画、ビデオクリップ）；
- (b) 攻撃的、わいせつ、又は犯罪的な内容、若しくは、当社又はクライアントに当惑を引き起こす可能性のある内容。
- (c) 個人又は組織に関する、虚偽の名誉毀損の声明。
- (d) 差別的、攻撃的、侮蔑的、又は他者を当惑させる可能性のある資料（機会均等ポリシー、ハラスメント防止、及びいじめに関するポリシーに違反する資料を含む。）。
- (e) 当社、当社のスタッフ又はクライアントに関する機密情報（職務の適切な遂行において許可されている場合を除く。）。
- (f) 許可されていないソフトウェア。

(g) (あなた又は当社にとって) 刑事または民事責任を引き起こす可能性のあるその他の声明。

(h) 著作権を侵害する音楽、ビデオファイル又はその他の素材。

Schedule 4 ソーシャルメディア方針

1. この方針について

- 1.1 このポリシーは、ソーシャルメディアの使用を通じて、当社のビジネスへのリスクを最小限に抑えるために実施されている。
- 1.2 このポリシーは、Facebook、LinkedIn、Twitter、Google+、Wikipedia [、Whisper] [、Instagram] [、Tumblr]、その他のすべてのソーシャルネットワーキングサイト、インターネット投稿、ブログなど、あらゆる形態のソーシャルメディアの使用を対象としている。これは、ビジネス目的でのソーシャルメディアの使用、及び当社のビジネスに何らかの影響を与える可能性のある個人的な使用に、適用される。
- 1.3 この方針は、従業員の雇用契約の一部を構成するものではなく、いつでも変更することができる。

2. ソーシャルメディアの個人利用

- 2.1 [ソーシャルメディアの個人的な使用は、勤務時間中である場合、若しくは、当社のコンピューター、ネットワーク、その他の IT リソース、及び通信システムを使用する場合、許可されない。]

または

[勤務時間中のソーシャルメディアの時折の個人的な使用は、それが非専門的、又は不適切なコンテンツを含まず、あなたの職責又は生産性を妨げず、このポリシーに合致している限り、許可される。]

3. 禁止される使用

- 3.1 間接的であっても、当社のビジネス上の利益や評判を損なう可能性のある、ソーシャルメディアコミュニケーションを行わないようにしなければならない。
- 3.2 当社、当社のスタッフ又は第三者を、名誉毀損したり、誹謗中傷するため、スタッフや第三者に対して、嫌がらせ、いじめ、又は不法な差別をするため、虚偽または誤解を招く発言をするため、若しくは、同僚や第三者になりすますため、ソーシャルメディアを使用してはならない。
- 3.3 上司から明示的に許可されていない限り、ソーシャルメディアを介して、当社に代わって意見を表明してはならない。そのような許可を取得するために、トレーニングを受ける必要がある。

- 3.4 当社の業績など、ビジネスに関連する機密性あるトピックについて、コメントを投稿したり、営業秘密、機密情報、知的財産を危険にさらすような行為を行ったりしてはならない。ソーシャルメディアへの投稿や、ソーシャルメディアのプロフィールに、当社のロゴやその他の商標を含めてはならない。
- 3.5 [雇用の過程で作成されたビジネス上の連絡先を、個人のソーシャルネットワーキングアカウントに追加することは、許されない。]

または

[あなたの雇用の過程で取得されたビジネス上の取引先の連絡先の詳細は、当社の機密情報にあたる。雇用終了時に、あなたは、そのようなすべての情報のコピーを、当社に提供し、あなたの個人的なソーシャルネットワーキングアカウントから、そのようなすべての情報を削除し、あなたが持っているかもしれない、そのような情報のさらなるコピーを破棄しなければならない。]

- 3.6 ソーシャルメディアの誤用は、[]に報告しなければならない。

4. **ソーシャルメディアの合理的な使用のためのガイドライン**

- 4.1 ソーシャルメディアの投稿または個人のプロフィールで、自分個人について話していることを明確にする必要がある。一人称で書いて、個人のメールアドレスを使用することとする。
- 4.2 ソーシャルメディアで発言するときは、他者に敬意を払い、インターネット上で、誰でも見ることができるように公開されるすべてのコミュニケーションについて、あなたが個人的に責任を負うことに注意しなければならない。
- 4.3 あなたが、あなたのプロフィール、又はソーシャルメディアの投稿で、当社との関係を開示する場合、あなたは、あなたの見解が、あなたの雇用主の見解を表していないことを表明しなければならない（3.3 に規定のように、当社に代わって話すことを許可されていない限り。）。また、プロフィールと投稿するコンテンツが、クライアントや同僚に提示する、職業上のイメージと一致していることを確認する必要がある。
- 4.4 あなたの意見や投稿の適切性について、確信が持てない、又は、懸念がある場合は、上司と話し合うまで投稿を控えなければならない。
- 4.5 当社を誹謗中傷したり、当社を悪く提示するソーシャルメディアコンテンツを見つけた場合は、[あなたのマネージャーまたは[部門]]に連絡する必要がある。

5. 本方針の違反

- 5.1 本方針の違反は、解雇を含む懲戒処分となりうる。[本方針の違反をしていると疑われるスタッフの者は、当社の調査に協力する必要がある。]
- 5.2 本方針に違反すると考えられるソーシャルメディアの内容を取り除くように求められることがある。除去の要求への不服従は、懲戒処分の対象になることがある。

Confidentiality Clause in Employment Agreement

11. Confidential Information

11.1 The Confidential Information means all confidential information relating to Employer [and its Group Company] that Employee obtain knowledge of, during the exercise of, or in connection with, Employee's duties owed to Employer [or its Group Company][, before, on or after the date of this agreement]. This includes:

- (a) all confidential or proprietary information relating to:
 - (i) the research and development plan, the business operation, the labor and employment, the marketing and advertising, the finance, submitted or received documents from regulatory authorities and other business partners, the past, present, and potential customers and clients, the affairs with customers and business affiliates [, OR or] plans and prospects[, intentions, or market opportunities] of Employer [or of the Employer's Group Company] that are not publicly known and not readily ascertainable by someone in the same or similar business circle; and
 - (ii) (the operations, processes, product information, know-how, technical information, designs, trade secrets, or software of Employer[, or of Employer's Group Company] that are indicated as proprietary information by Employer or its representative or its Group Company;
- (b) any information, findings, data or analysis derived from the Confidential Information; [and]
- (c) any other information that is identified by Employer or its Representatives [or its Group Company, or their Representatives] as being of a confidential or proprietary nature[; and OR .]
- (d) [any information detailed in Exhibit A]

but excludes any information referred to in clause 11.2.

11.2 Information is not the **Confidential Information** if:

- (a) it is, or becomes, generally available to the public other than as a direct or indirect result of the information being disclosed by Employee or its Representatives in breach of this agreement [(except that any compilation of otherwise public information in a form not publicly known shall still be treated as the Confidential Information)];
- (b) it was available to Employee on a non-confidential basis prior to disclosure by Employer;

- (c) it was, is, or becomes available to Employee on a non-confidential basis from a person who, to Employee's knowledge, is not under any confidentiality obligation in respect of that information;
- (d) it was lawfully in the possession of Employee before the information was disclosed by Employer; [or]
- (e) [it is developed by or for Employee independently of the information disclosed by Employer; or]
- (f) the parties agree in writing that the information is not confidential.

12. Confidential Obligations

12.1 Either during this agreement or at any time during [number] years after the termination of this agreement Employee shall:

- (a) keep the Confidential Information secret and confidential;
- (b) use the Confidential Information only during the exercise of Employee's duties owed to Employer;
- (c) maintain the label and classification of the Confidential Information as confidential in a manner that anyone who is exposed to the Confidential Information can understand the confidentiality of the Confidential Information all the time;
- (d) protect the Confidential Information with necessary care so that no one can misuse or access to the Confidential Information without authorization;
- (e) take security measures as set forth in Exhibit B;
- (f) not directly or indirectly disclose, make available, or attempt to disclose or make available, any Confidential Information in whole or in part to any person, except as expressly permitted by, and only necessary to perform Employee's duties, in accordance with this agreement;
- (g) not copy, reduce to writing or otherwise record the Confidential Information except as strictly necessary for the performance of Employee's duties. Any such copies, reductions to writing and records shall be the property of Employer[; and OR .];
- (h) not convey, disclose, or implicitly provide information about Employer's products and services and Employee's work in a lecture or a publication without obtaining a prior authorization from Employer;
- (i) immediately notify Employer of (1) any suspected actual or imminent breach of confidentiality by Employee, (2) any actual or imminent disclosure, security breach, misuse, misappropriation, or any other unauthorized use by any person including Permitted Disclosure and Mandatory Disclosure;
- (j) not obtain or attempt to obtain intellectual property rights on the Confidential Information

(k) [[INCLUDE ANY OTHER SPECIFIC REQUIREMENTS.]]

13. Permitted Disclosure

13.1 Employee may disclose the Confidential Information to its Representatives on the basis that it:

- (a) informs Employer's business affiliates, employees, and customers, of the confidential nature of the Confidential Information before it is disclosed; and
- (b) procures that those persons or entities comply with the confidentiality obligations in clause 12.1

14. Mandatory Disclosure

14.1 Subject to the provisions of this clause, Employee may disclose the Confidential Information to the minimum extent required by:

- (a) an order of any court of competent jurisdiction or any regulatory, judicial, governmental or similar body or any taxation authority of competent jurisdiction;
- (b) the laws or regulations of any country to which Employer [or its Group Company] is subject.

14.2 Before Employee discloses any Confidential Information pursuant to clause 14.1 Employee shall, to the extent permitted by law, use all reasonable endeavours to give Employer as much notice of this disclosure as possible.

15. Return or destruction of the Confidential Information

15.1 (1) Upon completion or termination of the employment, or (2) upon Employer's request at any time in writing to Employee, Employee shall:

- (a) return to Employer all documents, data, and materials [and any copies thereof] containing, reflecting, incorporating or based on Employer's Confidential Information;
- (b) return to Employer all documents, devices, data, and materials [and any copies thereof] which relate to Employer or its Group Company including notes, reports, memos, records, files, drawings, protocols, and other similar documents;
- (c) certify in writing to Employer that items listed in 5.1.(b) are the sole property of Employer and its Group Company and that Employee has complied with the requirements of this clause 15.1.

16. Reservation of rights and acknowledgment

- 16.1 Except as expressly stated in this agreement, Employer makes any express or implied warranty or representation concerning its Confidential Information, including but not limited to the accuracy or completeness of the Confidential Information.
- 16.2 The disclosure of the Confidential Information by Employer shall not form any offer by, or representation or warranty on the part of, Employer to enter into any further agreement with Employee.

17. Rights and remedies

- 17.1 Except as expressly provided in this agreement, the rights and remedies provided under this agreement are in addition to, and not exclusive of, any rights or remedies provided by law.
- 17.2 [Without prejudice to any other rights or remedies that each party may have, each party acknowledges and agrees that damages alone would not be an adequate remedy for any breach of the terms of this agreement by the other party. Accordingly, each party shall be entitled to the remedies of injunctions, specific performance or other equitable relief for any threatened or actual breach of this agreement.]

Exhibit A Designated Confidential Information

Exhibit B Minimum Security Measures

1. Protection and non-sharing of an ID, a badge, a key, a password, or any other form of authentication information that allows a holder's access to Employer's premises or log in to a device or equipment that may display or provide access to Confidential Information.
2. Locking of a device or equipment that may display or provide access to Confidential Information.
3. Limitation of printing on paper or other tangible medium for display, sharing, conveyance, retention, recording, saving, or any other types of use of Confidential Information
4. Prohibition of transferring, storing, saving, copying, recording, photographing, and duplicating of Confidential Information except authorized by Employer
5. Prohibition of a device and/or a means that possesses the functionality of copying, photographing, recording, transmitting, sharing, conveying, saving, or storing Confidential Information in premises and buildings where Employee uses or affords access to Confidential Information
6. Prohibition of use of Employee's own device and equipment for accessing or using Confidential Information
7. ...

英国：雇用契約中の機密保持条項

1. 機密情報

- 1.1 機密情報とは、従業員が、自己の雇用主〔及びそのグループ会社〕に対して負う職責を遂行する間に、又は、遂行に関連して、〔本合意の締結前、締結日、あるいは締結以降〕知ることとなった、雇用主〔及びそのグループ会社〕に関する機密性ある情報を意味する。これには、以下を含む。：
- a. 下記に関連するすべての機密情報、あるいは、保有情報：
 - (i) 公に知られておらず、同じか類似の業界の者が、容易に確認できない、雇用主〔、又は雇用主のグループ会社〕の、研究・開発計画、事業運営、労働及び雇用、マーケティング及び広告、財務、規制当局並びにその他のビジネスパートナーに提出された、若しくは受領した文書、過去、現在並びに将来の顧客及び取引相手、顧客並びに事業関連会社との関係〔、又は〕計画、及び、見通し〔、意図、若しくは、市場機会〕；
 - (ii) (雇用主、その代表者、又は、そのグループ会社によって保有情報として示される、雇用主〔、又は、雇用主のグループ会社〕の業務、プロセス、製品情報、ノウハウ、技術情報、デザイン、営業秘密、又は、ソフトウェア)；
 - b. 機密情報に由来する情報、発見、データ、又は、解析；〔及び〕
 - c. 雇用主〔、その代表者、又は、そのグループ会社〕によって、それが秘密で所有されることを指定された、その他の情報〔；または〕
 - d. 〔Exhibit A に記載の情報〕

が、次項 1.2. に言及された情報を除く。

1.2 次の情報は、機密情報にあたらぬ：

- a. 〔(公知の情報の、公に知られていない形態への編集が、機密情報として扱われるべきことを除き。)]、従業員、又は、その代理人が、この合意に反して開示したこと、直接、あるいは、間接の結果としてではなく、一般に入手可能である、又は、一般に入手可能となった；
- b. 雇用主から開示されるより前に、従業員が、機密保持義務なく入手可能であった；
- c. 従業員が知る限り、当該情報について機密保持義務を負わない人物から、従業員が、機密保持義務なく、入手が可能となった、可能である、又は、可能となる；

- d. 雇用主から開示される前に、従業員に合法に所持されていた；[又は]
- e. [雇用主から開示された情報と独立して、従業員により、又は、従業員のために開発された；又は]
- f. 当事者が、書面で、情報が機密情報ではないと合意した。

2. 機密保持義務

- 2.1 本契約中、又は、本契約の終了後[]年間、如何なる時点でも、従業員は：
 - a. 機密情報を秘密にして機密性を保持する；
 - b. 雇用主に対して負う職責を遂行する間にのみ、機密情報を使用する；
 - c. 機密情報に接する者が、機密情報の機密性を常に理解できるように、機密情報のラベル及び分類を、機密として維持する；
 - d. 誰も、機密情報を権限なく不正使用、又は、違法にアクセスできないように、必要な注意をもって、機密情報を保護する；
 - e. Exhibit B に指定のセキュリティ対策を実施する；
 - f. 本契約に従い、従業員の職責を遂行するのに必要な限度で、かつ、明示的に許可を得ている場合を除き、いずれの者に対しても、直接又は間接に、機密情報の全部又はその一部を、開示、利用可能化、又は、開示若しくは利用可能化の試みを行わない；
 - g. 従業員の職責を遂行するのに厳密に必要な場合以外、機密情報のコピー、文書化、あるいは記録化を行わない。作成されたコピー、文書、及び、記録は、いずれも雇用主の財産となる[；そして]；
 - h. 事前に雇用主から許可を得ることなく、講義や発表にて、雇用主の製品やサービス、及び、従業員の仕事に係る情報を、伝播、開示、又は、暗黙の提供を行わない；
 - i. (1) 現実の、又は、差し迫った、従業員による疑われる機密保持義務違反、(2) 許される開示及び強制的開示を含む、現実の、又は、差し迫った、何者かによる開示、安全性の侵害、不正使用、侵害、又は、その他の無許可の使用について、雇用主に直ぐに通知する；
 - j. 機密情報に関して、知的財産権を取得ないしは得ようとししない
 - k. [[その他の必要事項を含める]]

3. 許される開示

- 3.1 従業員は、以下の条件で、自己の代理人に対して、機密情報を開示することができる：

- a. 機密情報が開示される前に、雇用主の関連会社、従業員及び顧客に、機密情報の機密性を通知
- b. それらの個人又は団体が、2.1の機密保持義務を遵守することの取り付け

4. 強制的開示

- 4.1 本条項の規定するところにより、従業員は、要求された最小限度で、機密情報を開示することができる：
 - a. 管轄権を有する裁判所、規制庁、司法機関、行政庁若しくは他の同様の機関、又は管轄権を有する税務当局の命令；
 - b. 雇用主[、又はそのグループ会社]が服する法律、又は規制
- 4.2 4.1項に従い、従業員が機密情報を開示する前に、従業員は、法律で許される限度で、雇用主に、当該開示に関してできるだけ通知するよう、合理的な努力をしなければならない。

5. 機密情報の返還、又は、消去

- 5.1 (1) 雇用の完了、若しくは、終了に際して、又は、(2)何時でも、雇用主の、書面による従業員への要請により、従業員は：
 - a. 雇用主の機密情報を含んだ、反映した、取り込んだ、あるいは、基礎とする、全ての書面、データ、資料[、及び、それらのコピー]を、雇用主に返還することとする；
 - b. ノート、レポート、メモ、記録、ファイル、図面、プロトコル、及び、その他の同様の文書を含む、雇用主、又は、そのグループ会社に関連する、すべての文書、装置、データ、並びに、資料[、及び、それらのコピー]を、雇用主に返却する；
 - c. 従業員は、5.1.bの項目が、雇用主とそのグループ会社のための財産であり、従業員が5.1.の要件を充足したことを、雇用主に書面で確証する

6. 権利の保留及び確認

- 6.1 本合意で明示に規定されている場合を除き、雇用主は、機密情報の正確性、あるいは完全性に限られないが、それを含めて、機密情報に関する明示、若しくは、黙示の保証、又は、表明を行わない。
- 6.2 雇用主の機密情報の開示は、従業員とのさらなる合意を締結する、雇用主による申出、又は、雇用主の表明、若しくは、保証を構成しない。

7. 権利と救済

- 7.1 本合意で明示的に規定されている場合を除き、本合意に基づいて付与される権利、及び救済は、法律によって付与される権利、及び救済に追加されるものであり、これを排除するものではない。
- 7.2 [各当事者が持つ可能性のある、他の権利又は救済を妨げることなく、各当事者は、損害賠償だけでは、他の当事者による本合意内容の違反に対する適切な救済ではないことを認め、同意する。したがって、各当事者は、恐れのある、若しくは、現実の違反に対する差止命令、特定義務の履行、又は、その他の衡平法上の救済を受ける権利を有するものとする。]

Exhibit A

指定機密情報

Exhibit B

最小安全性措置

1. その保有者が、雇用主の施設にアクセスしたり、機密情報を表示、若しくは、アクセスすることのできる装置や機器に、ログインしたりすることを許す、ID、バッジ、キー、パスワード、又は、その他の形式の認証情報の、保護と非共有。
2. 機密情報を表示、又は、それにアクセスを付与する、装置、若しくは、機器の施錠・暗号化。
3. 機密情報の展示、共有、移転、保持、記録、保存、又は、その他の種類の使用のために利用される、紙やその他の有体媒体への印刷の制限。
4. 雇用主の許可がない限り、機密情報の転送、貯蔵、保存、コピー、記録、写真撮影、及び、複製の禁止。
5. 従業員が、機密情報を使用、若しくは、アクセスできる、施設、並びに建物での、機密情報のコピー、写真撮影、記録、送信、共有、伝達、保存、又は、貯蔵の機能を備えた装置、及び/又は、手段の禁止
6. 機密情報にアクセスする、又は使用するために、従業員個人の装置又は機器を使用することの禁止
7. . . .

3 退職後の競業禁止契約書の例

UK Employee Non-compete Agreement

1. Interpretation

The definitions and rules of interpretation in this clause apply in this agreement.

- a. **Board:** the board of directors of the Company (including any committee of the board duly appointed by it).
- b. **Capacity:** as agent, consultant, director, employee, worker, owner, partner or shareholder.
- c. **Confidential Information:** information (whether or not recorded in documentary form, or stored on any magnetic or optical disk or memory) which is not in the public domain relating to [our **OR** any Group Company's] business, products, affairs and finances for the time being confidential to [us **OR** any Group Company] and trade secrets including, without limitation, technical data and know-how relating to [our **OR** any Group Company's] business or any of [our **OR** its] business contacts, including in particular (by way of illustration only and without limitation) [EXAMPLES].
- d. **Garden Leave:** any period during which we have [exercised our rights under clause [NUMBER] **OR** required you not to do any work or contact our employees or business contacts].
- e. **[Group Company:** the Company, its Subsidiaries or Holding Companies from time to time and any Subsidiary of any Holding Company from time to time.]
- f. **Restricted Business:** those parts of [our **OR** any Group Company's] business with which you were involved to a material extent in the [PERIOD] months before Termination.
- g. **Restricted Customer:** any firm, company or person who, during the [PERIOD] months before Termination, was [a customer or prospective customer of **OR** in the habit of dealing with] [the Company **OR** any Group Company] with whom you had contact [or about whom you became aware or informed] in the course of your employment.
- h. **Restricted Person:** anyone employed [or engaged] by [us **OR** any Group Company] [at the level of [POSITION] or above and who could materially damage [our **OR** any Group Company's] interests if they were involved in any Capacity in any business concern which competes with any Restricted Business] and with whom you dealt in the [PERIOD] months before Termination in the course of your employment.
- i. **[Subsidiary and Holding Company:** in relation to a company mean "subsidiary" and "holding company" as defined in section 1159 of the Companies Act 2006 [and a company shall be treated, for the purposes only of the membership requirement contained in subsections 1159(1)(b) and (c), as a member of another company even if its shares in that other company are registered in the name of (a) another person (or its nominee), whether by way of security or in connection with the taking of security, or (b) a nominee].]
- j. **Termination:** the termination of your employment with us howsoever caused.

2. Restrictions

- 2.1 In order to protect the Confidential Information and [our **OR** any Group Company's] business connections to which you have access as a result of the your employment by us, you covenant with us [(on our own behalf and as trustee and agent for each Group Company)] that you shall not:
- a. during your employment by us and for [PERIOD] months after Termination, solicit or endeavour to entice away from [us **OR** any Group Company] the business or custom of a Restricted Customer with a view to providing goods or services to that Restricted Customer in competition with any Restricted Business;
 - b. [during your employment by us and for [PERIOD] months after Termination [in the course of any business concern which is in competition with any Restricted Business], offer to employ or engage or otherwise endeavour to entice away from [us **OR** any Group Company] any Restricted Person;]
 - c. [during your employment by us and for [PERIOD] months after Termination [in the course of any business concern which is in competition with any Restricted Business], employ or engage or otherwise facilitate the employment or engagement of any Restricted Person, whether or not such person would be in breach of contract as a result of such employment or engagement;]
 - d. during your employment by us and for [PERIOD] months after Termination, be involved in any Capacity with any business concern which is (or intends to be) in competition with any Restricted Business;
 - e. for [PERIOD] months after Termination, be involved with the provision of goods or services to (or otherwise have any business dealings with) any Restricted Customer in the course of any business concern which is in competition with any Restricted Business;
 - f. at any time after Termination, represent yourself as connected with [us **OR** any Group Company] in any Capacity, other than as a former employee, or use any registered names or trading names associated with [us **OR** any Group Company];
 - g. during your employment by us,
 - (i) disclose or use, or attempt to disclose or use, Confidential Information or trade secrets that you have access to, without written authorization, or allow directly or indirectly, an unauthorized third party to obtain or use Confidential Information or trade secrets;
 - (ii) pursue or attempt to pursue economic or social interest of any business concern other than us; or
 - h. during your employment by us, without written authorization,
 - (i) provide goods or services of, or carry out business activities (including consultation, financing, management, operation, and marketing) of, or engage in preparatory activities for the launch of,
 - (ii) assume a Capacity in,
 - (iii) assist employing or engaging an employee by, or
 - (iv) represent yourself as holding any Capacity in, or as connected with,

business concerns other than us.

2.2 None of the restrictions in clause 2.1 shall prevent you from:

- a. holding an investment by way of shares or other securities of not more than [5]% of the total issued share capital of any company, whether or not it is listed or dealt in on a recognised stock exchange; [or]
- b. being engaged or concerned in any business concern insofar as your duties or work shall relate solely to geographical areas where the business concern is not in competition with any Restricted Business[; or **OR** .]
- c. [being engaged or concerned in any business concern, provided that your duties or work shall relate solely to services or activities of a kind with which you were not concerned to a material extent in the [PERIOD] months before Termination.]

2.3 The restrictions imposed on you by this clause 2 apply to you acting:

- a. directly or indirectly; and
- b. on your own behalf or on behalf of, or in conjunction with, any firm, company or person.

2.4 The period[s] for which the restriction[s] in clause 2.1 apply shall be reduced by any period that you spend on Garden Leave immediately before Termination.

2.5 If, during the your employment by us or before the expiry of the last of the covenants in this clause 2, you receive an approach or offer to be involved in any Capacity in a business which competes with any part or parts of [our OR any Group Company's] business with which you are or have been involved to a material extent during the your employment by us, you shall:

- a. notify [us OR the Board] [in writing] of the fact of the approach or offer and the identity of the person making the approach or offer as soon as possible; [and]
- b. [if requested, provide a copy of any written offer as soon as possible; and]
- c. give the person making the offer a copy of this clause 2 within [seven days] of the offer being made.

The obligations contained in this clause 2.5 are continuing obligations and shall also apply if, at any time subsequent to the relevant approach or offer being made but before the expiry of the last of the covenants in this clause 2, the business making the offer or approach so competes with [our OR any Group Company's] business.

2.6 [If, at any time during your employment, [two] or more Restricted Persons have left their employment, appointment or engagement with us to carry out services for a business concern which competes with, or is intended to compete with any Restricted Business, you will not at any time during the six months following the last date on which any of those Restricted Persons were employed or engaged by us, be employed or engaged in any way with that business concern.]

2.7 The parties entered into the restrictions in this clause 2 having been separately legally advised.

- 2.8 Each of the restrictions in this clause 2 is intended to be separate and severable. If any of the restrictions shall be held to be void but would be valid if part of their wording were deleted, such restriction shall apply with such deletion as may be necessary to make it valid or effective.
- 2.9 If your employment is transferred to any firm, company, person or entity other than a Group Company (the "New Employer") pursuant to the Transfer of Undertakings (Protection of Employment) Regulations 2006, you will, if required, enter into an agreement with the New Employer containing post-termination restrictions corresponding to those restrictions in this clause 2, protecting the [confidential information], trade secrets and business connections of the New Employer.
- 2.10 [You will, at our request and expense, enter into a separate agreement with any Group Company in which you agree to be bound by restrictions corresponding to those restrictions in this clause 2 (or such of those restrictions as may be appropriate) in relation to that Group Company.]

従業員の競業禁止条項

1. 解釈

本条項における定義と解釈の規則は、本契約に適用される。

- a. **取締役会**：当社の取締役会（正式に任命された、取締役会の委員会を含む。）。
- b. **地位**：エージェント、コンサルタント、ディレクター、従業員、労働者、所有者、パートナー、又は株主として。
- c. **機密情報**：[当社又はグループ会社の]事業、製品、商務及び財務に関連する、パブリックドメインにない情報（文書形式で記録されているかどうか、及び、磁気又は光学ディスク、若しくは、メモリに保存されているかどうかにかかわらず。）で、[当社又はグループ会社に、]期間中機密であるもの、並びに、営業秘密（[当社又はグループ会社]の事業に関連する技術データ及びノウハウ、若しくは、当社の[その]事業の連絡先を含むがこれらに限定されない。）、特に（説明のためのみで、制限されない。）[例]。
- d. **ガーデンリープ**：当社が、[第[数字]条に基づいて権利を行使した、若しくは、就労、又は、当社の従業員やビジネスの連絡先との連絡をやめるよう要求した]、期間。
- e. **[グループ会社]**：会社、その子会社、又は持ち株会社、及び、持ち株会社の子会社。]
- f. **制限ビジネス**：退職前の[期間]ヶ月間に重要な範囲で関与した[当社又はグループ会社の]ビジネスの部分。
- g. **制限顧客**：解雇前の[期間]ヶ月間に、[当社又はグループ会社][の顧客又は潜在的顧客であった、又は、と取引慣行にあった]、貴殿が、貴殿の雇用の過程で、コンタクトを取った、[若しくは、貴殿が知ようになった、又は、知らされた]事業所、会社、又は、個人。
- h. **制限対象者**：[当社又はグループ会社]によって[[地位]以上のレベルで雇用[又は従事]され、制限ビジネスと競合する事業主に、いかなる役割であっても関与する場合には、[当社又はグループ会社]の利益に重大な損害を与える可能性のあり]、かつ、貴殿が、雇用の過程で、退職の[期間]ヶ月内にやりとりした者。
- i. **[子会社及び持ち株会社]**：会社に関連して、2006 年会社法の第 1159 条で定義されている、「子会社」および「持ち株会社」を意味する。[そして、会社は、第 1159 条第(1) (b) 及び(c)に含まれる、メンバーシップ要件の目的でのみ、他の会社のメンバーとして扱われる。それは、他の会社の株式が(a)証券によるか、又は、証券を獲得することに関連してかにかかわらず、他者（又はその被指名人）の名前で、若しくは、(b)被指名人の名前で、登録されている場合でも当てはまる。]
- j. **退職**：いかなる原因であれ、当社と貴殿との間の雇用の終了。

2. 制約

- 2.1 雇用の結果として貴殿がアクセスできる機密情報及び[当社又はグループ会社の]ビジネス上のつながりを保護するために、以下の行為に及ばないことを、当社に合意する[（当社自身のため、各グループ会社の受託者及び代理人として）]：
- a. 退職後[期間]の期間、制限ビジネスと競合する商品又はサービスを提供する目的で、制限顧客を勧誘をして、[当社又はグループ会社]から、制限顧客のビジネス又は取引慣行を、奪い取る、又は、奪い取るように努めること。
 - b. [退職後[期間]の期間]、[制限ビジネスと競合する事業主の関連で]、制限対象者を雇用又は採用するか、その他の方法で、[当社又はグループ会社]から、引き抜こうと努めること。]
 - c. [退職後[期間]、[制限ビジネスと競合する事業主の関連で]、制限対象者が、雇用又は採用されることで、契約違反となるかどうかにかかわらず、制限対象者を雇用又は採用するか、若しくは、雇用又は採用を援助すること。
 - d. 退職後から[期間]ヶ月間、制限ビジネスと競合している（又は競合する予定の）事業主で、地位に就くこと。
 - e. 退職後[期間]の期間、制限ビジネスと競合する事業主の関連で、制限顧客への商品又はサービスの提供に関与する（、若しくは、その他の方法で、ビジネスを行う）こと。
 - f. 退職後いつでも、元従業員以外の何らかの地位で、[当社又はグループ会社と]関係があることを表明するか、[当社又はグループ会社]に関連する登録名称又は商号を使用すること。
 - g. 雇用中、
 - (i) 貴殿がアクセスできる機密情報又は営業秘密を、当社の書面による許可なく、開示又は使用、若しくは、開示又は使用の試みをする、あるいは、直接又は間接に、当社により許可を受けていない第三者が、機密情報又は営業秘密を取得あるいは使用できるようにすること、
 - (ii) 当社以外の事業主の経済的又は社会的利益を追求する、若しくは、追求しようとする。
 - h. 雇用中、当社の書面による許可なく、当社以外の他の事業主の、
 - (i) 商品又はサービスの提供に関与する、若しくは、そのビジネス活動（顧問、ファイナンス、経営、運営、及び、販売促進を含む）又は開業準備を行うこと、
 - (ii) 地位に就くこと、
 - (iii) 従業員の雇用又は採用を援助すること、

(iv)地位に就いている、又は、関係があると表明すること。

2.2 前項 2.1 の制限は、以下を妨げない。

- a. 公認の証券取引所に上場又は取引されているかどうかにかかわらず、会社の発行済み株式資本合計の[5]%以下の株式又はその他の証券による投資を保有すること。
- b. 職責又は仕事が、制限ビジネスと競合しない地理的領域に限定される限りで、事業主の事業に従事する、あるいは、関与する[;又は]
- c. [貴殿の義務又は仕事が、終了前の[期間]月間に重要な範囲で関与しなかった種類のサービス又は活動に限られることを条件として、事業主の事業に従事する、又は関与すること。]

2.3 第 2 条による制限は、貴殿の下記行動に適用される：

- a. 直接的、又は、間接的；
- b. 貴殿個人、事業所、会社、又は、他者のために、若しくは、それらと連携して

2.4 前 2.1 項の制限が適用される期間は、退職直前にガーデンリープに服した間だけ、短縮される。

2.5 雇用中、又は、第 2 条の規定の各制約が最後に満了する前に、貴殿が雇用中に重要な範囲で関与している、又は関与したことがある、[当社又はグループ会社の]事業の一部又は複数の部分と競合する、事業の地位に貴殿が就くかという、接触又は申出を受け取った場合、以下をしなければならない：

- a. [当社又は取締役会]に、[書面で]、接触又は申出の事実と、接触又は申出を行った者の身元を、できるだけ直ぐに通知する。
- b. [要求に応じて、書面による申出のコピーを、できるだけ直ぐに提供する。]
- c. 申出をした者に、申出が行われてから[7 日]以内に、この第 2 条のコピーを渡す。

第 2.5 項に含まれる義務は、継続的な義務であり、関連する接触又は申出が行われた後で、第 2 条の各制約が最後に満了する前に、申出又は接触を行う事業主が、[当社又はグループ会社]の事業と競合する場合に、適用される。

2.6 [貴殿の雇用中の任意の時点で、[2]人以上の制限対象者が、制限ビジネスと競合する、又は競合することを企図する事業主の、サービス実現のために、雇用される、任命される、又は、採用を離れる場合、これら制限対象者のいずれかが、当社によって雇用又は採用された最後の日から 6 か月間、貴殿は、その事業主に、何らかの形で雇用される、若しくは、従事してはならない。]

2.7 両当事者は、独立した法的助言を受けた上で、第 2 条の制限に合意した。

- 2.8 第 2 条の各制限は、別個で、分離できることを意図している。制限のいずれかが無効とみなされても、それらの文言の一部が削除されると有効である場合、当該制限は、それを有効化する、又は、効力をもたせる必要な削除とともに適用される。
- 2.9 2006 年事業譲渡（雇用の保護）規則に従って、グループ会社以外の事業所、会社、個人、又は団体（「新規雇用主」という。）に雇用が譲渡された場合、[機密情報]、営業秘密、及び、新規雇用主のビジネス上のつながりを保護するため、第 2 条の制限に対応する退職後の制限を含め、必要に応じて、新規雇用主と合意する。
- 2.10 [当社の求めに応じて、当社の費用で、グループ会社に対して、別個に、この第 2 条の規定する制限に対応した制限（又は、その中で適切と考えられるな制限）に拘束されることに同意する。]

Confidentiality Clause in Transactional Agreements

18. Confidential Information

18.1 The Confidential Information means all confidential information relating to the Purpose which Discloser or its Representatives [or its Group Company, or their Representatives] directly or indirectly provides to Recipient or its Representatives [or its Group Company, or their Representatives][, before, on or after the date of this agreement]. This includes:

- (a) the fact that discussions and negotiations are taking place concerning the Purpose and the status of those discussions and negotiations;
- (b) [the [existence and] terms of this agreement;]
- (c) all confidential or proprietary information relating to:
 - (i) the research and development, the business operations, the finance, the past, present, and potential customers and clients, the affairs with customers and business affiliates[, OR] plans[, intentions, or market opportunities] of Discloser [or of Discloser's Group Company] that are not publicly known and not readily ascertainable by someone in the same or similar business circle; and
 - (ii) (the operations, processes, product information, know-how, technical information, designs, trade secrets or software of Discloser[, or of Discloser's Group Company] that are indicated as proprietary information by Discloser or its representative or its Group Company;
- (d) any information, findings, data or analysis derived from the Confidential Information; [and]
- (e) any other information that is identified by Discloser or its Representatives [or its Group Company, or their Representatives] as being of a confidential or proprietary nature[; and OR .]
- (f) [any information detailed in Exhibit A]

but excludes any information referred to in clause 11.2.

18.2 Information is not the **Confidential Information** if:

- (a) it is, or becomes, generally available to the public other than as a direct or indirect result of the information being disclosed by Recipient or its Representatives in breach of this agreement [(except that any compilation of otherwise public information in a form not publicly known shall still be treated as the Confidential Information)];

- (b) it was available to Recipient on a non-confidential basis prior to disclosure by Discloser;
- (c) it was, is, or becomes available to Recipient on a non-confidential basis from a person who, to Recipient's knowledge, is not under any confidentiality obligation in respect of that information;
- (d) it was lawfully in the possession of Recipient before the information was disclosed by Discloser; [or]
- (e) [it is developed by or for Recipient independently of the information disclosed by Discloser; or]
- (f) the parties agree in writing that the information is not confidential.

19. Confidential Obligations

19.1 In return for Discloser making the Confidential Information available to Recipient, Recipient undertakes to Discloser that it shall:

- (a) keep the Confidential Information secret and confidential;
- (b) not use the Confidential Information except when it is necessary to realize the Purpose;
- (c) label and classify the Confidential Information as confidential in a manner that anyone who is exposed to the Confidential Information can understand the confidentiality of the Confidential Information all the time;
- (d) protect the Confidential Information with necessary care so that no one can misuse or access to the Confidential Information without authorization;
- (e) take security measures as set forth in Exhibit B;
- (f) not directly or indirectly disclose, make available, or attempt to disclose or make available, any Confidential Information in whole or in part to any person, except as expressly permitted by, and only necessary to realize the Purpose, in accordance with this agreement;
- (g) obtain a valid confidentiality agreement in writing from any employee, officer, expert, business affiliate, and person who are expected to receive or be exposed to the Confidential Information and legally bind such employee, officer, expert, business affiliate, and person with duty of confidentiality identical to Recipient's duty of confidentiality under this agreement;
- (h) obtain written consent from Discloser to any contractual or statutory transfer of Recipient's contractual rights and/or duties under this agreement, prior to transfer of such rights and/or duties;
- (i) not copy, reduce to writing or otherwise record the Confidential Information except as strictly necessary for the Purpose. Any such copies, reductions to writing and records shall be the property of Discloser[; and OR .];

- (j) immediately notify Discloser of (1) any suspected actual or imminent breach of confidentiality by Recipient or its employee, officer, expert, business affiliate, and other person who are expected to receive or be exposed to the Confidential Information, (2) any actual or imminent disclosure, security breach, misuse, misappropriation, or any other unauthorized use by any person including Permitted Disclosure and Mandatory Disclosure;
- (k) not obtain or attempt to obtain intellectual property rights on the Confidential Information
- (l) [[INCLUDE ANY OTHER SPECIFIC REQUIREMENTS.]]

20. Permitted Disclosure

- 20.1 Recipient may disclose the Confidential Information to its Representatives on the basis that it:
- (a) informs those Representatives of the confidential nature of the Confidential Information before it is disclosed; and
 - (b) procures that those Representatives comply with the confidentiality obligations in clause 12.1 as if they were Recipient.
- 20.2 Recipient shall be liable for the actions or omissions of the Representatives in relation to the Confidential Information as if they were the actions or omissions of Recipient.

21. Mandatory Disclosure

- 21.1 Subject to the provisions of this clause, a party may disclose the Confidential Information to the minimum extent required by:
- (a) an order of any court of competent jurisdiction or any regulatory, judicial, governmental or similar body or any taxation authority of competent jurisdiction;
 - (b) the rules of any listing authority or stock exchange on which its shares [or those of its Group Company] are listed or traded; or
 - (c) the laws or regulations of any country to which its affairs [or those of its Group Company] are subject.
- 21.2 Before a party discloses any Confidential Information pursuant to clause 14.1 it shall, to the extent permitted by law, use all reasonable endeavours to give the other party as much notice of this disclosure as possible. [Where notice of such disclosure is not prohibited and is given in accordance with clause 14.2, that party shall take into account the reasonable requests of the other party in relation to the content of this disclosure.]
- 21.3 If a party is unable to inform the other party before the Confidential Information is disclosed pursuant to clause 14.1 it shall, to the extent permitted by law, inform the other party of the full

circumstances of the disclosure and the information that has been disclosed as soon as reasonably practicable after such disclosure has been made.

22. Return or destruction of the Confidential Information

22.1 (1) Upon completion or termination of the Purpose and (2) upon Discloser's request at any time in writing to Recipient, Recipient shall:

- (a) destroy [or return to Discloser] all documents and materials [(and any copies)] containing, reflecting, incorporating or based on Discloser's Confidential Information;
- (b) erase all Discloser's Confidential Information from its computer and communications systems and devices used by it, or which is stored in electronic form; [and]
- (c) [[to the extent technically and legally practicable,] erase all Discloser's Confidential Information which is stored in electronic form on systems and data storage services provided by third parties; and]
- (d) certify in writing to Discloser that it has complied with the requirements of this clause 15.1.

22.2 Nothing in clause 15.1 shall require Recipient to return or destroy any documents and materials containing or based on Discloser's Confidential Information that Recipient is required to retain by applicable law, or to satisfy the requirements of a regulatory authority or body of competent jurisdiction or the rules of any listing authority or stock exchange, to which it is subject. The provisions of this agreement shall continue to apply to any documents and materials retained by Recipient pursuant to this clause 22.2.

23. Reservation of rights and acknowledgment

23.1 The disclosure of the Confidential Information by one party does not give the other party or any other person any licence or other right in respect of any Confidential Information beyond the rights expressly set out in this agreement.

23.2 Except as expressly stated in this agreement, Discloser makes any express or implied warranty or representation concerning its Confidential Information, including but not limited to the accuracy or completeness of the Confidential Information.

23.3 The disclosure of the Confidential Information by the parties shall not form any offer by, or representation or warranty on the part of, that party to enter into any further agreement with the other party [in relation to the Purpose].

24. Rights and remedies

- 24.1 Except as expressly provided in this agreement, the rights and remedies provided under this agreement are in addition to, and not exclusive of, any rights or remedies provided by law.
- 24.2 [Without prejudice to any other rights or remedies that each party may have, each party acknowledges and agrees that damages alone would not be an adequate remedy for any breach of the terms of this agreement by the other party. Accordingly, each party shall be entitled to the remedies of injunctions, specific performance or other equitable relief for any threatened or actual breach of this agreement.]

25. No obligation to continue discussions

Nothing in this agreement shall impose an obligation on either party to continue discussions or negotiations in connection with the Purpose, or an obligation on each party[, or its Group Company] to disclose any information (whether the Confidential Information or otherwise) to the other party.

26. Ending Discussions and duration of confidentiality obligations

- 26.1 If either party decides not to continue to be involved in the Purpose with the other party, it shall notify that other party in writing immediately.
- 26.2 Notwithstanding the end of discussions between the parties in relation to the Purpose pursuant to clause 26.1, each party's obligations under this agreement shall continue in full force and effect for a period of [two] years from the date of this agreement.
- 26.3 The end of discussions relating to the Purpose shall not affect any accrued rights or remedies to which either party is entitled.

Exhibit A Designated Confidential Information

Exhibit B Minimum Security Measures

8. Password requirement for logging into a device that may display or provide access to Confidential Information to a user of the device.
9. Limitation of printing on paper or other tangible medium for display, sharing, conveyance, retention, recording, saving, or any other types of use of Confidential Information
10. Limitation of access to premises and buildings where Recipient uses or affords access to Confidential Information to only those who owe duty of confidentiality to Recipient
11. Prohibition of a device and/or a means that possesses the functionality of copying, photographing, recording, transmitting, sharing, conveying, saving, or storing Confidential Information in premises and buildings where Recipient uses or affords access to Confidential Information
12. . . .

英国：取引関係相手との機密保持条項

1. 機密情報

1.1 機密情報とは、開示者若しくはその代表者[又はそのグループ会社若しくはその代表者]が、受領者若しくはその代表者[又はそのグループ会社若しくはその代表者]に[本件契約前、締結時、又は締結以降]、直接又は間接的に提供する、すべての機密情報を意味する：

- (a) 本件契約の話し合い及び交渉が、その目的と現況に関して、行われているという事実；
- (b) [本件契約の[存在及び]条件；]
- (c) 以下に関連するすべての機密情報、又は保有情報：
 - (i) 公に知られておらず、同じか類似の業界の何者かが、容易に確認できない、開示者[、又は開示者のグループ会社]の、研究・開発計画、事業運営、財務、過去、現在、並びに、将来の顧客とクライアント、顧客並びにビジネスアフィリエイトとの関係[、又は]計画[、意図、又は市場機会]；
 - (ii) 開示者、その代表者、又はそのグループ会社によって保有情報として示される、開示者[、又は、開示者のグループ会社]の業務、プロセス、製品情報、ノウハウ、技術情報、デザイン、営業秘密、又は、ソフトウェア；
- (d) 機密情報に由来する情報、発見、データ、又は、解析；[そして]
- (e) 開示者、その代表者[、そのグループ会社、又はその代表者]によって、それが機密であるか、保有されることが、指定された、その他の情報
[；そして]
- (f) [Exhibit Aに記載の情報]

が、次項 1.2. に言及された情報を除く。

1.2 次の情報は、機密情報にあたらぬ：

- (a) [(公知の情報が公に知られていない形態への編集が機密情報として扱われるべきことを除き。)]、受領者、又は、その代理人が、この合意に反して開示したことの、直接、あるいは、間接の結果としてではなく、一般に入手可能である、又は、一般に入手可能となった；

- (b) 開示者から開示されるより前に、受領者が、機密保持義務なく入手可能であった；
- (c) 受領者が知る限り、当該情報について機密保持義務を負わない人物から、受領者が、機密保持義務なく、入手が可能となった、可能である、又は、可能となる；
- (d) 開示者から開示される前に、受領者に合法に所持されていた；[又は]
- (e) [開示者から開示された情報と独立して、受領者により、又は、受領者のために開発された；又は]
- (f) 当事者が、書面で、情報が機密情報ではないと合意した。

2. 機密保持義務

2.1 開示者が、機密情報を受領者が利用できるようにするのと引き換えに、受領者は、開示者に対して、以下を誓約する：

- (a) 機密情報を秘密にして機密性を保持する；
- (b) 目的を実現する必要がある場合を除き、機密情報を使用しない；
- (c) 機密情報に接する者が、機密情報の機密性を常に理解できるように、機密情報のラベル、及び、分類を、機密として維持する；
- (d) 誰も、機密情報を権限なく不正使用、若しくは、違法にアクセスできないように、必要な注意をもって、機密情報を保護する；
- (e) 別紙 B に記載されているセキュリティ対策を講じる；
- (f) 本契約に従い、目的の実現に必要な限度で、かつ、明示の許可を得ている場合を除き、いずれの者に対しても、直接若しくは間接に、機密情報の全部若しくはその一部を、開示、利用可能化、又は、開示や利用可能化の試みを行わない；
- (g) 従業員、役員、専門家、ビジネスアフィリエイト、及び、機密情報を受信又は接することが予想される人物から、本契約に基づく受領者の機密保持義務と同一の機密保持義務をそのような人物に課す有効な機密保持契約を書面で取得する；
- (h) 本契約に基づく、受領者の契約上の権利及び/若しくは義務の、契約上又は法定の譲渡について、そのような権利及び/若しくは義務の譲渡の前に、開示者から書面による同意を得る；
- (i) 目的のために厳密に必要な場合を除き、機密情報をコピー、文書化、その他の記録化を行わない。作成されたコピー、文書、及び、記録は、いずれも開示者の財産となる[；そして]；

- (j) (1) 現実の、若しくは、差し迫った、受領者、その従業員、役員、専門家、ビジネスアフィリエイト、及び、機密情報を受け取るか、又は、機密情報に接することが予想されるその他の人物による、機密保持義務違反の疑い、(2) 許される開示、並びに、強制的開示を含む、現実の、若しくは、差し迫った、何者かによる開示、安全性の侵害、不正使用、侵害、又は、その他の無許可の使用について、開示者に直ちに通知する；
- (k) 機密情報に関して、知的財産権を取得、ないしは、得ようとする
- (1) [[その他の必要事項を含める]]

3. 許される開示

- 3.1 受領者は、以下の条件で、自己の代理人に対して、機密情報を開示することができる：
 - 1) 機密情報が開示される前に、それら代理人に、機密情報の機密性を通知
 - 2) それらの代理人が、受領者のように、2.1 の機密保持義務を遵守することの取り付け
- 3.2 受領者は、機密情報に関連する、代理人の作為又は不作為について、あたかも受領者自身の作為又は不作為であるかのように、責任を負う。

4. 強制的開示

- 4.1 本条項の規定するところにより、当事者は、要求された最小限度で、機密情報を開示することができる：
 - (a) 管轄権を有する裁判所、規制庁、司法機関、行政庁、若しくは、他の同様の機関、又は、管轄権を有する税務当局の命令；
 - (b) その株式（又はそのグループ会社の株式）が上場又は取引されている上場当局又は証券取引所の規則；
 - (c) その業務（又はそのグループ会社の業務）が適用される国の法律又は規制
- 4.2 4.1 に従い、当事者が機密情報を開示する前に、法律で許される限度で、相手当事者に、当該開示に関してできるだけ通知するよう、合理的な努力をしなければならない。[そのような開示の通知が禁止されておらず、4.2 項に従って行われる場合、その当事者は、この開示の内容に関する相手当事者の合理的な要求を、考慮に入れる。]

- 4.3 4.1 項に従って機密情報が開示される前に、当事者が相手当事者に通知できない場合、法律で許可されている範囲で、その開示が行われた後、合理的に可能な限り直ぐに、開示の全状況及び開示された情報を、相手当事者に通知する。

5. 機密情報の返還、又は、消去

- 5.1 (1)目的の完了、若しくは、終了に際して、又は、(2)何時でも、開示者の、書面による受領者への要請により、受領者は：
- (a) 開示者の機密情報を含んだ、反映した、取り込んだ、あるいは、基礎とする、全ての書面及び資料[、及び、それらのコピー]を、破棄[、又は、開示者に返還]することとする；
 - (b) 自己のコンピュータと通信システム、及び、自己が使用するデバイスに存在する、又は電子形式で保存されている、すべての開示者の機密情報を消去する；
 - (c) [技術的及び法的に実行可能な範囲で]、第三者が提供するシステム及びデータストレージサービスに電子形式で保存されている、開示者の全機密情報を消去する；
 - (d) この条項 5.1 の要件に適合していることを、開示者に書面で確証する。
- 5.2 第 5.1 項のいかなる規定も、適用される法により、受領者が保持する必要がある、あるいは、規制当局又は管轄機関の要求、若しくは、対象となる上場当局又は証券取引所の規則を満たす必要のある、開示者の機密情報を含む、又は、それに基づく、文書及び資料を返却又は破棄することを、受領者に要求するものではない。本契約の規定は、本項 5.2 に従って受領者が保持する、すべての文書及び資料に、引き続き適用されるものとする。
- ## 6. 権利の保留及び確認
- 6.1 一方の当事者による機密情報の開示は、本契約で明示的に定められた権利を超えて、他方の当事者又は他者に、機密情報に関するライセンス又はその他の権利を与えるものではない。
- 6.2 本合意で明示に規定されている場合を除き、開示者は、機密情報の正確性又は完全性に限られないが、それを含めて、機密情報に関する、明示、若しくは、黙示の保証、又は、表明を行わない。
- 6.3 当事者の機密情報の開示は、[目的に関して、]相手当事者とのさらなる合意を締結する、当事者による申出、又は、当事者の表明、若しくは、保証を構成しない。

7. 権利及び救済

- 7.1 本合意で明示的に規定されている場合を除き、本合意に基づいて付与される権利、及び、救済は、法律によって付与される権利、及び、救済に追加されるものであり、これを排除するものではない。
- 7.2 [各当事者が持つ可能性のある、他の権利又は救済を妨げることなく、各当事者は、損害賠償だけでは、他の当事者による本合意内容の違反に対する、適切な救済ではないことを認め、同意する。したがって、各当事者は、恐れのある、若しくは、現実の違反に対する差止命令、特定義務の履行、又は、その他の衡平法上の救済を受ける権利を有するものとする。]

8. 話し合いを続ける義務の不存在

本契約のいかなる条項も、いずれかの当事者に、目的に関連して話し合い、若しくは、交渉を継続する義務を課すことはなく、各当事者[又はそのグループ会社]に情報（機密情報又はその他）を他方当事者に開示する義務を課すことはない。

9. 話し合いの終了及び守秘義務の期間

- 9.1 いずれかの当事者が、他方の当事者との目的に関与し続けないと決めた場合、直ちに、書面で、他方当事者に通知するものとする。
- 9.2 9.1 項に基づく、目的に関する当事者間の話し合いの終了にもかかわらず、本契約に基づく各当事者の義務は、本契約の日付から[2]年間、完全に効力を持ち続ける。
- 9.3 目的に関する話し合いの終了は、いずれかの当事者が有する、未払いの権利又は救済に影響を与えない。

Exhibit A

指定機密情報

1. ユーザーに、機密情報を表示、又は、機密情報へのアクセスを提供する可能性のある装置にログインするためのパスワードの要求。
2. 機密情報の展示、共有、移転、保持、記録、保存、又は、その他の種類の使用のために利用される、紙やその他の有体媒体への印刷の制限。
3. 受領者が機密情報を使用する、又は、機密情報へのアクセスを許可する、施設及び建物へのアクセスを、受領者に機密保持義務を負っている者のみに制限。
4. 受領者が、機密情報を使用、若しくは、機密情報へのアクセスを提供する、施設、並びに建物での、機密情報のコピー、写真撮影、記録、送信、共有、伝達、保存、又は、貯蔵の機能を備えた装置、及び/又は、手段の禁止
5. . . .

5 来訪者受付表

Visitor List

No.	Name	ID	Contact details	Company	Arrival	Departure	Accepted by

(参考和訳)来訪者受付表

訪問客リスト

No.	氏名	本人確認	連絡先	所属団体	到着日 時	出発日 時	受入対応者 (受入先)

報告書の利用についての注意・免責事項

本報告書は、日本貿易振興機構（ジェトロ）が現地調査会社に委託し作成したものであり、調査後の法律改正などによって情報が変わる場合があります。掲載した情報・コメントは調査委託先の判断によるものであり、情報の正確性や一般的な解釈がこのとおりであることを保証するものではありません。また、本報告書はあくまでも参考情報の提供を目的としており、法的助言を構成するものではなく、法的助言として依拠すべきものではありません。本報告書にてご提供する情報等に基づいて行為をされる場合には、必ず個別の事案に沿った具体的な法的助言を別途お求め下さい。

ジェトロおよび調査委託先は、本報告書の記載内容に関して生じた直接的、間接的、派生的、特別の、付随的、あるいは懲罰的な損害および利益の喪失について、それが契約、不法行為、無過失責任、あるいはその他の原因に基づき生じたかにかかわらず、一切の責任を負いません。これは、たとえジェトロまたは調査委託先が係る損害等の可能性を知らされていても同様とします。

[調査受託]

Brundidge & Stanger, P.C.

独立行政法人 日本貿易振興機構 ニューヨーク事務所

2022年3月

禁無断転載

本報告書の作成においては、できるだけ正確な情報の提供を心がけておりますが、本報告書で提供している情報は、調査時点で入手・判明し得たものであり、ご利用に際してはこの点をご留意の上、ご活用ください。